Juniper Networks
Steel-Belted Radius

Installation and Upgrade Guide

Release 6.1
January 2008

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: SBR-TD-GS61 Revision 02

Copyright © 2004–2007 Juniper Networks, Inc. All rights reserved. Printed in USA.

Steel-Belted Radius, Juniper Networks, the Juniper Networks logo are registered trademark of Juniper Networks, Inc. in the United States and other countries. Raima, Raima Database Manager and Raima Object Manager are trademarks of Birdstep Technology. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Portions of this software copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California All Rights Reserved Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions of this software copyright © 2001-2002, Networks Associates Technology, Inc All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software are copyright © 2001-2002, Cambridge Broadband Ltd. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software copyright © 1995-2002 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

- The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
- Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
- This notice may not be removed or altered from any source distribution.

HTTPClient package Copyright © 1996-2001 Ronald Tschalär (ronald@innovation.ch).

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. For a copy of the GNU Lesser General Public License, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

StrutLayout Java AWT layout manager Copyright © 1998 Matthew Phillips (mpp@ozemail.com.au).

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details. For a copy of the GNU Lesser General Public License, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

M0817

Table of Contents

About This Guide vii
Audience ... vii
What's In This Manual ... vii
Typographical Conventions ... viii
Editions/Used In ... viii
Syntax ... ix
Related Documentation ... ix
Steel-Belted Radius Documentation ... ix
Requests for Comments (RFCs) ... x
Third-Party Products ... xi
Contacting Technical Support ... xi

Chapter 1 Overview 1
Steel-Belted Radius Features ... 1
Release Highlights ... 2
Release 6.1 ... 2
Release 6.0 ... 3
Release 5.4 ... 4
Release 5.3 ... 5
Licensing ... 5

Chapter 2 Preparing for Installation 7
Review the Release Notes ... 7
Select a Server ... 7
Verify System Requirements ... 8
System Requirements – Windows ... 8
System Requirements – Solaris ... 10
System Requirements – Linux ... 11
Verify Network Connectivity ... 13
Verify Host Name Resolution ... 13
Verify Administrator Account Access ... 14
Obtain a Server License Number ... 14

Chapter 3 Windows Installation 15
Before You Begin ... 15
Installing the Steel-Belted Radius Server Software ... 15
Upgrading from a 30-Day Trial Installation ... 18
Upgrading from Steel-Belted Radius Version 6.0 or 5.4 ... 19
Uninstall the SBR Version 5.4 Administrator ... 23
Restoring a Previous Configuration ... 23
Stopping the Steel-Belted Radius Service ... 23
Starting the Steel-Belted Radius Service ... 24

Chapter 4 Solaris Installation 25

Before You Begin 25
Upgrade Files 26
Package Management Commands 26
Installing the Steel-Belted Radius Server Software 27
Next Steps 32
Upgrading from a 30-Day Trial Installation 33
Upgrading from Steel-Belted Radius Versions 6.0 or 5.4 34
Before You Begin 34
Begin the Upgrade Procedure 39
Next Steps 45
Additional Required Manual File Upgrades 46
Uninstall the SBR Version 5.4 Administrator 47
Restoring a Previous Configuration 48
Starting the RADIUS Server 49
Stopping the RADIUS Server 49
Displaying RADIUS Status Information 49

Chapter 5 Linux Installation 51
Before You Begin 51
Upgrade Files 52
Package Management Commands 52
Installing the Steel-Belted Radius Server Software 53
Next Steps 57
Upgrading from a 30-Day Trial Installation 58
Upgrading from Steel-Belted Radius Versions 6.0 or 5.4 59
Before You Begin 59
Begin the Upgrade Procedure 64
Use dbconvert to Migrate the btrieve Database to the raima Database 67
Finalize the Upgrade Procedure 69
Additional Required Manual File Upgrades 73
Uninstall the SBR Version 5.4 Administrator 74
Moving Steel-Belted Radius to another Operating System 75
Moving Configuration Data to Another Operating System 76
Upgrading in Place to Another Operating System 78
Starting the RADIUS Server 78
Stopping the RADIUS Server 79
Displaying RADIUS Status Information 79

Chapter 6 Verifying Native User Authentication 81
Before You Begin 81
Configuring the Server 81
Verifying Native User Authentication 82
Downloading the RadiusTest Utility 82
Installing the RadiusTest Utility 83
Configuring Steel-Belted Radius 83
Configuring the RadiusTest Utility 85

Chapter 7 Uninstalling Steel-Belted Radius 89
Uninstalling on Windows 89
Uninstalling the Steel-Belted Radius Server 89
Uninstalling the SBR Administrator Files 89
Uninstalling on Solaris 90
Uninstalling the Steel-Belted Radius Server 90
Uninstalling the SBR Administrator Files 91

Uninstalling on Linux 92
Uninstalling the Steel-Belted Radius Server 92
Uninstalling the SBR Administrator Files 93
Glossary **95**
Index **101**

About This Guide

The *Steel-Belted Radius Installation and Upgrade Guide* describes how to install or upgrade the Steel-Belted Radius software on a server running the Solaris operating system, the Linux operating system, or the Windows XP/Windows Server 2003 operating system.

Audience

This manual is intended for network administrators who are responsible for implementing and maintaining authentication, authorization, and accounting services for an enterprise. This manual assumes that you are familiar with general RADIUS and networking concepts and the specific environment in which you are installing Steel-Belted Radius.

If you use Steel-Belted Radius with third-party products such as Oracle or RSA SecurID, you should be familiar with their installation, configuration, and use.

What's In This Manual

This manual contains the following chapters and appendixes:

- Chapter 1, "Overview," presents an overview of Steel-Belted Radius and describes installation and licensing requirements for Steel-Belted Radius.
- Chapter 2, "Preparing for Installation," describes the tasks that you should complete before you install Steel-Belted Radius.
- Chapter 3, "Windows Installation," describes how to install the Steel-Belted Radius server software on a Windows host.
- Chapter 4, "Solaris Installation," describes how to install the Steel-Belted Radius server software on a Solaris host.
- Chapter 5, "Linux Installation," describes how to install the Steel-Belted Radius server software on a Linux host.
- Chapter 6, "Verifying Native User Authentication," describes how to configure basic settings and native users in Steel-Belted Radius and how to use the RadiusTest utility to verify that Steel-Belted Radius can authenticate a native user.

- Chapter 7, “Uninstalling Steel-Belted Radius,” describes how to uninstall the Steel-Belted Radius server software and the SBR Administrator from a Windows, Solaris, or Linux host.
- The Glossary provides brief explanations for RADIUS terminology used in this and other Steel-Belted Radius manuals.

Typographical Conventions

Table 1 describes the text conventions used throughout this manual.

Table 1: Typographical Conventions

Convention	Description	Examples
Bold typeface	Indicates buttons, field names, dialog names, and other user interface elements.	Use the **Scheduling** and **Appointment** tabs to schedule a meeting.
Plain sans serif typeface	Represents: ■ Code, commands, and keywords ■ URLs, file names, and directories	Examples: ■ Code: certAttr.OU = 'Retail Products Group' ■ URL: Download the JRE application from: http://java.sun.com/j2se/
Italics	Identifies: ■ Terms defined in text ■ Variable elements ■ Book names	Examples: ■ Defined term: An *RDP client* is a Windows component that enables a connection between a Windows server and a user’s machine. ■ Variable element: Use settings in the **Users** > **Roles** > *Select Role* > **Terminal Services** page to create a terminal emulation session. ■ Book name: See the *Steel-Belted Radius Administration Guide.*

Editions/Used In

Steel-Belted Radius is available in multiple editions to meet the requirements of different types of customers. This manual uses the following abbreviations to identify editions of Steel-Belted Radius:

- GEE: Global Enterprise Edition
- SPE: Service Provider Edition
- SPE + EAP: Service Provider Edition with optional EAP Extension Module
- EE: Enterprise Edition

Syntax

- *radiusdir* represents the directory into which Steel-Belted Radius has been installed. By default, this is C:\Program Files\Juniper Networks\Steel-Belted Radius for Windows systems and /opt/JNPRsbr/radius on Linux and Solaris systems.

- Brackets [ ] enclose optional items in format and syntax descriptions. In the following example, the first *Attribute* argument is required; the syntax indicates you can include an optional second *Attribute* argument by entering a comma and the second *Attribute* argument (without the square brackets) on the same line.

  <add | replace> = *Attribute* [,*Attribute*]

  In configuration files, brackets identify section headers:

  the [Processing] section of proxy.ini

  In screen prompts, brackets indicate the default value. For example, if you press Enter without entering anything at the following prompt, the system uses the indicated default value (/opt).

  Enter install path [/opt]:

- Angle brackets < > enclose a list from which you must choose an item in format and syntax descriptions.

- A vertical bar (|) separates items in a list of choices. In the following example, you must specify add or replace (but not both):

  <add | replace> = *Attribute* [,*Attribute*]

Related Documentation

The following documents supplement the information in this manual.

Steel-Belted Radius Documentation

Please review the ReleaseNotes.txt file that accompanies your Steel-Belted Radius software. This file contains the latest information about features, changes, known problems, and resolved problems. If the information the ReleaseNotes.txt file differs from the information found in the Steel-Belted Radius manuals, use the information in the ReleaseNotes.txt file.

In addition to this manual, the Steel-Belted Radius documentation includes the following manuals:

- The *Steel-Belted Radius Reference Guide* describes the configuration files and settings used by Steel-Belted Radius.

- The *Steel-Belted Radius Administration Guide* describes how to configure and administer the Steel-Belted Radius software.

- The *Steel-Belted Radius LDAP Scripting Guide* describes how to use scripts written in the JavaScript programming language to enhance the search capabilities of the Steel-Belted Radius LDAP Authentication module.

Requests for Comments (RFCs)

The Internet Engineering Task Force (IETF) maintains an online repository of Request for Comments (RFC)s online at http://www.ietf.org/rfc.html. Table 2 lists the RFCs that apply to this guide.

Table 2: Related RFCs

RFC Number	Title
RFC 1155	*Structure and Identification of Management Information for TCP/IP-based Internets*. M. Rose, K. McCloghrie, May 1990.
RFC 1213	*Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*. K. McCloghrie, M. Rose, March 1991.
RFC 2271	*An Architecture for Describing SNMP Management Frameworks*. D. Harrington, R. Presuhn, B. Wijnen, January 1998.
RFC 2284	*PPP Extensible Authentication Protocol (EAP)*. L. Blunk, J. Volbrecht, March 1998.
RFC 2433	*Microsoft PPP CHAP Extensions*. G. Zorn, S. Cobb, October 1998.
RFC 2548	*Microsoft Vendor-specific RADIUS Attributes*. G. Zorn. March 1999.
RFC 2607	*Proxy Chaining and Policy Implementation in Roaming*. B. Aboba, J. Vollbrecht, June 1999.
RFC 2618	*RADIUS Authentication Client MIB*. B. Aboba, G. Zorn. June 1999.
RFC 2619	*RADIUS Authentication Server MIB*. G. Zorn, B. Aboba. June 1999.
RFC 2620	*RADIUS Accounting Client MIB*. B. Aboba, G. Zorn. June 1999.
RFC 2621	*RADIUS Accounting Server MIB*. G. Zorn, B. Aboba. June 1999.
RFC 2622	*PPP EAP TLS Authentication Protocol*. B. Aboba, D. Simon, October 1999.
RFC 2809	*Implementation of L2TP Compulsory Tunneling via RADIUS*. B. Aboba, G. Zorn. April 2000.
RFC 2865	*Remote Authentication Dial In User Service (RADIUS)*. C. Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.
RFC 2866	*RADIUS Accounting*. C. Rigney. June 2000.
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*. G. Zorn, B. Aboba, D. Mitton. June 2000.
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*. G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret. June 2000.
RFC 2869	*RADIUS Extensions*. C. Rigney, W. Willats, P. Calhoun. June 2000.
RFC 2882	*Network Access Servers Requirements: Extended RADIUS Practices*. D. Mitton. July 2000.
RFC 3162	*RADIUS and IPv6*. B. Aboba, G. Zorn, D. Mitton. August 2001.
RFC 3575	*Internet Assigned Numbers Authority (IANA) considerations for Remote Authentication Dial In User Service (RADIUS)*. B. Aboba, July 2003.
RFC 3579	*RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)*. B. Aboba, P. Calhoun, September 2003.
RFC 3580	*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*. P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, September 2003.

Third-Party Products

For more information about configuring your access servers and firewalls, consult the manufacturer's documentation that is provided with each device.

Contacting Technical Support

For technical support, open a support case using the Case Manager link at http://www.juniper.net/support/ or call 1-888-314-JTAC (from the United States,Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Check our website (http://www.juniper.net) for additional information and technical notes. When you are running SBR Administrator, you can choose **Web > Steel-Belted Radius User Page** to access a special home page for Steel-Belted Radius users.

When you call technical support, please have the following information at hand:

- Your Steel-Belted Radius product edition and release number (for example, Global Enterprise Edition version 6.1).
- Information about the server configuration and operating system, including any OS patches that have been applied.
- For licensed products under a current maintenance agreement, your license or support contract number.
- Question or description of the problem, with as much detail as possible.
- Any documentation that can help resolve the problem, such as error messages, memory dumps, compiler listings, and error logs.

Chapter 1

Overview

Thank you for selecting the Steel-Belted Radius® software. Steel-Belted Radius is a complete implementation of the RADIUS (Remote Authentication Dial In User Service) protocol that runs in your Windows, Solaris, or Linux environment. It interfaces with a wide variety of network access equipment, and authenticates remote and WLAN users against numerous back-end databases — enabling you to consolidate the administration of your remote and WLAN users, however they connect to your network. Steel-Belted Radius records usage statistics in an accounting database, so you can track and document user sessions for accounting and billing purposes.

Steel-Belted Radius Features

- Centralized management of user access control and security.
- Flexible authentication options let you use your existing OS-based authentication database, token-based authentication systems, and external SQL/LDAP databases for remote and WLAN user authentication.
- Support for a wide variety of 802.1X-compliant network access devices ensures compatibility in your network environment.
- Flexible, powerful proxy RADIUS features let you easily distribute authentication and accounting requests to the appropriate RADIUS server for processing.
- High-performance operation guarantees speedy internet access, with no waiting by the customer.
- **GEE/SPE**: Advanced external authentication features let you authenticate against multiple, redundant SQL or Lightweight Directory Access Protocol (LDAP) databases according to configurable load balancing and retry strategies, ensuring the highest level of service delivery to your users.
- **GEE/SPE**: You can control the time periods during which each user is allowed access. An access request is granted only during a user's allowed access hours; otherwise it is refused, even if the user presents valid credentials.
- **GEE/SPE**: You can define and apply administrative access levels to user or group accounts on the server machine. You can apply read, write, and read/write access selectively to different categories of configuration data.

- **GEE/SPE**: Auto-restart permits the Steel-Belted Radius server to restart itself automatically if it experiences a shutdown.
- **GEE/SPE**: Advanced proxy features let you easily authenticate users against RADIUS servers at other sites.
  - You have a choice of user name format, and you can configure routing based on user name decoration, dialed number identification service (DNIS), or specific attributes.
  - You can selectively modify attributes as proxy packets flow to and from Steel-Belted Radius.
  - You can specify groups of proxy target servers that handle proxy requests according to load-balancing or retry strategies — for the best performance and reliability.
- **GEE/SPE**: Directed authentication and accounting features simplify the hosting of RADIUS services by allowing Steel-Belted Radius to provide different services for each of your customers. Incoming requests can be directed to specific authentication or accounting methods based on user name decoration or DNIS.
- **GEE/SPE**: Your choice of interface lets you configure Steel-Belted Radius by means of a graphical SBR Administrator program or by means of LDAP (either programmatically or at the command line prompt).
- **Solaris and Linux only:** SNMP support lets you centrally monitor Steel-Belted Radius from your SNMP console, in the same manner as you monitor other devices and services on your network. Steel-Belted Radius offers full SNMP support including SNMP traps and alarms.
- **Windows only**: Perfmon counter and Windows event support let you centrally monitor Steel-Belted Radius using platform tools, in the same manner as you monitor other services on your network.

Release Highlights

Release 6.1

Release 6.1 of the Steel-Belted Radius software includes the following changes:

- Standards-based login communication—SBR Administrator uses HTTPS instead of a proprietary protocol for login requests. If the Steel-Belted Radius server does not have a current server certificate, the server generates a new self-signed server certificate.
- Certificate revocation list (CRL) cache and proxy enhancements—Certificate processing has been improved in Release 6.1 in several respects:
  - Support for CRL cache flushing
  - CRL cache timeout

  - Enforcement of CRL serial numbers
  - CRL proxy connection settings
  - Proxy exclusion list
  - CCM replication
- Support for background CCM replication
- Replication backup and restore
- Daylight savings time—Release 6.1 adds support for automatic adjustment of system clock for daylight savings time. Additionally, users can choose between local time and UTC (coordinated universal time) for timestamps in the event log file.
- Configurable error handling for backend databases—Users can now specify whether errors should cause a disconnect/reconnect to a MySQL, ODBC, or Oracle database.
- New database—Steel-Belted Radius is now based on the Birdstep RDMe database. Users who are upgrading from previous releases of Steel-Belted Radius may have to do some manual data conversion depending on the operating system they are running.
- Operating system changes— Release 6.1 drops support for RedHat Linux ES/AS version 3.*x* and for all versions of SuSE Linux.

Release 6.0

Release 6.0 of the Steel-Belted Radius software included the following changes:

- Web-delivered SBR Administrator—The SBR Administrator configuration application is downloaded through a web browser from the Steel-Belted Radius server without requiring a permanent installation. You can download and run instances of SBR Administrator from multiple Steel-Belted Radius servers simultaneously.
- Operating system changes—Release 6.0 adds support for RedHat Linux ES/AS version 4.*x*, SuSE Linux version 10.x. Solaris 8 and Windows 2000 are no longer supported.
- Oracle 10g—Release 6.0 adds support for Oracle 10g. Note that Steel-Belted Radius interoperates with Oracle 10g by means of the native OCI on Solaris, by means of JDBC on Linux and Solaris, and by means of ODBC on Windows.
- Location-based profiles (GEE/SPE only)—Release 6.0 adds support for assigning profiles to users based on the network access device through which the user is accessing a network.
- Location groups—Release 6.0 adds support for grouping of network access devices to simplify administration of location and profile rules.

- Audit logs—Release 6.0 adds support for administration audit logs that identify administrator logins/logouts, changes made during an administration session, and results of replication attempts.
- EAP configuration through SBR Administrator—Release 6.0 adds support for configuration of EAP methods and certificates through the SBR Administrator.
- Filter configuration through SBR Administrator—Release 6.0 adds support for management of filters used by tunneled EAP methods and proxy/directed realms (GEE/SPE only) through the SBR Administrator.
- Certificate confirmation—Release 6.0 allows an administrator to confirm that a certificate is associated with a user or host through the SBR Administrator.
- Support for TLS and AD accounts—On Windows servers, EAP-TLS can verify the presence of a user's certificate in Active Directory.
- Realm scripting and attribute filtering (GEE/SPE only)—A separately licensed scripting module lets you provide scripts that select a realm for processing for a particular request and filter the attributes of a particular request. Scripts can independently query databases and LDAP directories.

Release 5.4

Release 5.4 of the Steel-Belted Radius software included changes to the following:

- File permissions for log files (Solaris/Linux)—You can specify user and group file permissions for Steel-Belted Radius log files to control who can read them.
- Address ranges for RADIUS clients—If you have a number of RADIUS clients with contiguous IP addresses, you can define a RADIUS client entry with a range of IP addresses. All clients with addresses in that range, including clients added later, can send RADIUS requests.
- Operating system changes—Steel-Belted Radius supports Solaris 10. Windows NT is no longer supported.
- Optional null terminator in reply attributes—A setting in the radius.ini file controls whether Steel-Belted Radius sends reply attributes of type string without a null terminator.
- Simplified CCM upgrades—The procedure for upgrading servers in a Centralized Configuration Management realm is simplified, allowing your primary server to remain the primary throughout.
- Master dictionary overrides—By default, inbound proxy responses use the master dictionary when assigning values to attributes. You can cause the RADIUS client's dictionary to be used instead, by specifying the UseMasterDictionary parameter in radius.ini or in a .pro or .dir file.
- High-resolution timestamps in logs—You can have higher-resolution time stamps in the RADIUS log if you specify LogHighResolutionTime = yes in the [Configure] section of radius.ini.

Release 5.3

Release 5.3 of the Steel-Belted Radius software included the following changes:

- Centralized Configuration Management—Release 5.3 adds support for Centralized Configuration Management (CCM).
- EAP-EOTP and EAP-POTP support—Release 5.3 adds support for the Extensible Authentication Protocol-Extended One-Time Password (EAP-EOTP/EAP-15) and EAP-Protected One-Time Password (EAP-POTP/EAP-32) authentication with the SecurID authentication method.
- Package-based installation—Release 5.3 adds support for package-based installation of the Steel-Belted Radius software.

Licensing

If you want to install the Steel-Belted Radius server software for a 30-day evaluation, you do not need a license key.

If you want to install a permanent (non-evaluation) copy of the Steel-Belted Radius server software, you must have a single-seat software license key.

If you have more than one copy of the Steel-Belted Radius server software installed, you must have a site license key, or you must have a separate license key for each installation.

The SBR Administrator can be downloaded to as many workstations as you require. The SBR Administrator does not require a license key.

For details about licensing, please refer to the Steel-Belted Radius license agreement or contact Juniper Networks.

Chapter 2

Preparing for Installation

This chapter describes the tasks you should complete before you install Steel-Belted Radius.

Review the Release Notes

The Steel-Belted Radius release notes contain important late-breaking information, such as known software problems and documentation corrections. Please review the release notes that accompany your Steel-Belted Radius software before you install or upgrade Steel-Belted Radius to ensure you are informed about important information not found elsewhere.

Select a Server

Select an appropriate host to run the Steel-Belted Radius server software. An appropriate RADIUS server has the following properties:

- Secure physical location—Network security begins with physical security. Without a secure physical location, such as a locked server room, your authentication server's security can be compromised, resulting in compromises to network security.
- Root access on the host limited to the system administrator—You should restrict logon access to the Steel-Belted Radius server to system administrators and others who need it. Ideally, the server should have no (or few) user accounts.
- Adequate memory and disk space—See "Verify System Requirements" on page 8 for information on hardware and software requirements.
- Administrative interface not accessible from outside your network—If your Steel-Belted Radius server has one network connection, limit access to the ports Steel-Belted Radius uses for configuration and administration.

  If your Steel-Belted Radius server has more than one network connection, the network connection used to configure and administer Steel-Belted Radius should be on an administrative network that is physically separate from other networks.

- Server does not run public network services such as FTP or HTTP—Running public network services or applications unrelated to user authentication on the Steel-Belted Radius server may adversely affect the performance of Steel-Belted Radius, since it must compete with other services and applications for the server's CPU resources. Moreover, running public network services on the authentication server potentially opens the server to malicious attacks.

- Server uses secure shared secret—The shared secret configured for Steel-Belted Radius protects all communications to and from the server, including session keys for wireless data encryption. You should configure shared secrets that are long enough and random enough to resist attack, and you should avoid using the same shared secret throughout your network. To maximize the security of your server's shared secret, consider using Juniper Network's free Password Amplifier utility, which takes an ordinary shared secret or password (swordfish) and hashes it repeatedly to produce a 16-character amplified secret (g8QvQuRgRsl1AQ1E). You can paste this amplified secret to your server configuration to maximize security.

  For more information on the free Password Amplifier utility, see http://www.juniper.net/customers/support/products/aaa_802/sbr_user.jsp.

- File permissions are set appropriately—If your Steel-Belted Radius software is running on a Solaris or Linux server, you should set file permissions to limit access to configuration, accounting, and log files used by Steel-Belted Radius. You can configure default file permissions for Steel-Belted Radius files in the sbrd.conf file. Optionally, you can override the default file permissions specified in the sbrd.conf file for individual log files.

  For information on setting permissions for Steel-Belted Radius files, refer to the *Steel-Belted Radius Administration Guide*.

Verify System Requirements

This section describes the hardware and software requirements for running Steel-Belted Radius on the Windows, Solaris, or Linux operating system.

System Requirements – Windows

The Steel-Belted Radius for Windows server software package includes the server software, various dictionary and database files to support authentication, and the SBR Administrator application, which provides an administration user interface.

Table 3: Windows Server – System Requirements

Operating system	■ Windows XP Workstation ■ Windows Server 2003
Networking	TCP/IP must be configured.
Memory	The Steel-Belted Radius server software requires a host with at least 256 megabytes of working memory (512 megabytes for servers with more than 10,000 RADIUS users.) The SBR Administrator requires a host with at least 256 megabytes of memory.

Table 3: Windows Server – System Requirements (continued)

Disk space	The Steel-Belted Radius server software requires approximately 200 - 400 megabytes of local (not NFS) disk space; hard disk space requirements for running Steel-Belted Radius depend on your system's product configuration. The SBR Administrator requires approximately 80 megabytes of local disk space.
Monitor	The SBR Administrator requires a monitor that supports 256+ colors.
Web browser	SBR Administrator works with the following browsers: ■ Microsoft Internet Explorer 6.0, 6.1, or 7.0 ■ Firefox 2.0.0, 2.0.0.1 ■ Mozilla 1.4, 1.6, 1.7 Your browser must be running the Java Runtime Environment (JRE) version 1.4.2 or later. You can download JRE software from http://java.sun.com. Refer to your browser documentation for information on how to install and configure your web browser.
Database (optional)	The Windows version of Steel-Belted Radius supports any SQL database server that is Open Database Connectivity (ODBC) compliant for RADIUS authentication and accounting. Although Oracle versions 9.0.0, and 10.0.0 are supported, versions 9.2.0 and 10.2.0.3 are recommended. If your Steel-Belted Radius server runs on Windows and you use stored procedures, you should use the Oracle 9i client.
Adobe Reader (optional)	If you want to display the Steel-Belted Radius manuals (PDF files) online, you must have version 6.0 or later of the Adobe Reader software installed on your workstation. The free Adobe Reader software can be downloaded from http://www.adobe.com. Refer to the Adobe Reader documentation for information on how to download and install the Adobe Reader software.
Firewall (optional)	Hardware or software firewalls, such as Microsoft Firewall, may interfere with the operation of Steel-Belted Radius. If your network includes a firewall, you should create exceptions to pass some or all of the following ports: ■ TCP 667 – LDAP Configuration Interface (LCI) port (required if you use the LCI) ■ TCP 1812 – Steel-Belted Radius control port ■ TCP 1813 – SBR Administrator port ■ UDP 1645 – Legacy RADIUS authentication port ■ UDP 1646 – Legacy RADIUS accounting port ■ UDP 1812 – IETF RADIUS authentication port ■ UDP 1813 – IETF RADIUS accounting port ■ UDP *port range* – Proxy RADIUS source port range (specified in the http://www.juniper.net/customers/support/products/aaa_802/sbr_user.jsp file. Default is 1024–65535.) To create port exceptions in Windows Firewall, choose **Start > Control Panel > Windows Firewall.** When the Windows Firewall window opens, click the **Exceptions** tab, click the **Add Port** button, and enter the name, port number, and port type for each port you want to include in the exception list.

System Requirements – Solaris

The Steel-Belted Radius for Solaris server software package includes the server daemon, various dictionary and database files to support authentication, and the SBR Administrator application, which provides an administration user interface.

Table 4: Solaris Server – System Requirements

Hardware	Sun UltraSPARC workstation or equivalent
Operating system	■ Sun Solaris 9 SPARC Platform Edition 8/03 (or later) ■ Sun Solaris 10 SPARC Platform Edition 3/05 (or later) The following patches (or better) are required for Solaris 9: ■ 112874-37 libc ■ 112963-25 ld.so.1 ■ 111711-16 libC 32-bit ■ 111712-16 libC 64-bit ■ 117560-03 libmtsk ■ 111722-05 libm ■ 115697-02 mtmalloc The following patches (or better) are recommended, but not required, for Solaris 9: ■ 112785-56 X11 6.6.1: Xsun ■ 113886-28 OpenGL 1.3 32-bit for J2SE ■ 113887-28 OpenGL 1.3 64-bit for J2SE ■ 113096-03 X11 6.6.1: OWconfig for J2SE The following patches (or better) are required for Solaris 10: ■ 120900-04 libzonecfg ■ 121133-02 zoneadm ■ 119254-28 patchadd ■ 119578-22 FMA patch for J2SE ■ 118822-30 kernel patch for J2SE ■ 118833-24 kernel patch ■ 120753-02 libmtsk ■ 119963-07 libC The following patches (or better) are recommended, but not required, for Solaris 10: ■ 121620-02 MediaLib
Desktop manager	Gnome2-metacity or CDE-dtwm
Memory	At least 256 megabytes of working memory (512 megabytes for servers with more than 10,000 RADIUS users.) The SBR Administrator requires a host with at least 256 megabytes of memory.
Disk space	The Steel-Belted Radius server software requires 325–650 megabytes of local (not NFS) disk space; hard disk space requirements for running Steel-Belted Radius depend on your system's product configuration. The Solaris version of SBR Administrator requires at least 81 megabytes of local disk space.
Monitor	The SBR Administrator requires a monitor that supports 256+ colors.
Networking	TCP/IP must be configured.

Table 4: Solaris Server – System Requirements (continued)

Perl	Perl version 5.8.3 is required if you want to use the auto-restart feature of Steel-Belted Radius. Earlier and later versions of Perl may cause problems. If you install version 5.8.3 of Perl on Solaris, you do not need to overwrite the Sun-supplied version at /usr/bin/perl, However, the first line of the radiusd script must specify the Perl executable that corresponds to version 5.8.3. For example, if Perl 5.8.3 is installed as /usr/local/bin/perl, then the first line of the radiusd script must specify: #!/usr/local/bin/perl.
Database (optional)	The Solaris version of Steel-Belted Radius supports any SQL database server that is Open Database Connectivity (ODBC) compliant for RADIUS authentication and accounting. Although Oracle versions 9.0.0 and 10.0.0 are supported, versions 9.2.0 and 10.2.0.3 are recommended. Oracle 10 typically requires a patch for Oracle bug 4516865 to correct the installed Oracle file access modes. The JDBC plug-in has been tested with MySQL running on Solaris or Linux, Oracle running on Solaris or Linux, and MSSQL.
Web browser	SBR Administrator works with the following browsers on all Solaris versions: ■ Mozilla 1.4, 1.6, 1.7 Your browser must be running the Java Runtime Environment (JRE) version 1.4.2 or later. You can download JRE software from http://java.sun.com. Refer to your browser documentation for information on how to install and configure your web browser.
Adobe Reader (optional)	If you want to display the Steel-Belted Radius manuals (PDF files) online, you must have version 6.0 or later of the Adobe Reader software installed on your workstation and have an appropriate value specified in your PATH variable. The free Adobe Reader software can be downloaded from www.adobe.com. Refer to the Adobe Reader documentation for information on how to download and install the Adobe Reader software.
Firewall (optional)	Hardware or software firewalls may interfere with the operation of Steel-Belted Radius. If your network includes a firewall, you should create exceptions to pass some or all of the following ports: ■ TCP 667 – LDAP Configuration Interface (LCI) port (required if you use the LCI) ■ TCP 1812 – Steel-Belted Radius control port ■ TCP 1813 – SBR Administrator port ■ UDP 1645 – Legacy RADIUS authentication port ■ UDP 1646 – Legacy RADIUS accounting port ■ UDP 1812 – IETF RADIUS authentication port ■ UDP 1813 – IETF RADIUS accounting port ■ UDP *port range* – Proxy RADIUS source port range (specified in the radius.ini file. Default is 1024–65535.)

System Requirements – Linux

The Steel-Belted Radius for Linux server software package includes the server daemon, various dictionary and database files to support authentication, and the SBR Administrator application, which provides an administration user interface.

Table 5: Linux Server – System Requirements

Hardware	Intel *X*86 workstation or server

Table 5: Linux Server – System Requirements (continued)

Operating system	■ RedHat Enterprise Linux ES 4.0 ■ RedHat Enterprise Linux AS 4.0 The server must run glibc 2.3.2 or 2.3.3, which is present by default in the supported versions of RedHat Linux.
Memory	At least 256 megabytes of working memory (512 megabytes for servers with more than 10,000 RADIUS users.) The SBR Administrator requires a host with at least 256 megabytes of memory.
Disk space	The Steel-Belted Radius server software requires 235–470 megabytes of local (not NFS) disk space; hard disk space requirements for running Steel-Belted Radius depend on your system's product configuration. The Linux version of SBR Administrator requires at least 88 megabytes of local disk space.
Monitor	The SBR Administrator requires a monitor that supports 256+ colors.
Networking	TCP/IP must be configured.
Perl	Perl (version 5.8.3) is required if you want to use the auto-restart feature of Steel-Belted Radius. Earlier and later versions of Perl may cause problems. The first line of the radiusd script must specify the Perl executable that corresponds to version 5.8.3. For example, if Perl 5.8.3 is installed as /usr/local/bin/perl, then the first line of the radiusd script must specify: #!/usr/local/bin/perl.
Database (optional)	The JDBC plug-in has been tested with MySQL running on Solaris or Linux, Oracle running on Solaris or Linux, and MSSQL.
Web browser (optional)	SBR Administrator works with the following browsers on all Linux platforms: ■ Firefox 2.0.0, 2.0.0.1 ■ Mozilla 1.4, 1.6, 1.7 ■ Konqueror 3.2.1, 3.3.1, 3.4, 3.5.1 Your browser must be running the Java Runtime Environment (JRE) version 1.4.2 or later. You can download JRE software from http://java.sun.com. Refer to your browser documentation for information on how to install and configure your web browser.
Adobe Reader (optional)	If you want to display the Steel-Belted Radius manuals (PDF files) online, you must have version 6.0 or later of the Adobe Reader software installed on your workstation and have an appropriate value specified in your PATH variable. The free Adobe Reader software can be downloaded from www.adobe.com. Refer to the Adobe Reader documentation for information on how to download and install the Adobe Reader software.

Table 5: Linux Server – System Requirements (continued)

Firewall (optional)	Hardware or software firewalls may interfere with the operation of Steel-Belted Radius. If your network includes a firewall, you should create exceptions to pass some or all of the following ports: ■ TCP 667 – LDAP Configuration Interface (LCI) port (required if you use the LCI) ■ TCP 1812 – Steel-Belted Radius control port ■ TCP 1813 – SBR Administrator port ■ UDP 1645 – Legacy RADIUS authentication port ■ UDP 1646 – Legacy RADIUS accounting port ■ UDP 1812 – IETF RADIUS authentication port ■ UDP 1813 – IETF RADIUS accounting port ■ UDP *port range* – Proxy RADIUS source port range (specified in the radius.ini file. Default is 1024–65535.)

Verify Network Connectivity

Use the ping command to verify that the server on which you are going to install Steel-Belted Radius can communicate with other devices, such as remote access servers, database servers, DHCP servers, DNS servers, and management workstations, on your network, over your TCP/IP network.

```
C:\> ping 192.168.12.54

Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
Reply from 192.168.12.54: bytes=32 time=7ms TTL=255
```

If the ping command fails, verify that the IP address of the remote host is correct, that the remote host is operational, and that all routers between your server and the remote host are operational.

Verify Host Name Resolution

The server on which you are going to install Steel-Belted Radius must have a stable, accessible IP address that is mapped in /etc/hosts or the Domain Name System (DNS) server to a resolvable hostname.

To verify that the server has a resolvable hostname, use the ping command with the server's hostname:

```
C:\> ping foo.juniper.net

Pinging foo.juniper.net [192.168.12.21] with 32 bytes of data:
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
Reply from 192.168.12.21: bytes=32 time=7ms TTL=255
```

Verify Administrator Account Access

You must have administrator (Windows)/root (Solaris/Linux) access to the server on which you are going to install the Steel-Belted Radius server software.

Obtain a Server License Number

If you want to install the Steel-Belted Radius server software for a 30-day evaluation, you do not need a license number.

If you want to install a single permanent (non-evaluation) copy of Steel-Belted Radius, you must have a single-seat software license number.

If you have more than one copy of the Steel-Belted Radius software installed, you must have either a separate license key for each installation or a site license key.

The SBR Administrator may be deployed on as many workstations as you require. The SBR Administrator does not require a license number.

For details about licensing, please refer to the Steel-Belted Radius license agreement or contact Juniper Networks.

Chapter 3

Windows Installation

This chapter describes how to install or upgrade the Steel-Belted Radius server software on a Windows domain controller, server, or workstation.

Before You Begin

- Verify that the proposed installation host complies with the hardware and software requirements of Steel-Belted Radius. For more information, see "System Requirements – Windows" on page 8.
- If you are upgrading an existing installation, back up your root and server certificates, and verify you know the password for your server certificate.
- Microsoft IAS (Internet Authentication Service) cannot be configured on the same server as Steel-Belted Radius. If Microsoft IAS is running on the server on which you are planning to install Steel-Belted Radius, disable it.
- The Steel-Belted Radius service should run under a local account. By default, Steel-Belted Radius runs as a local system account. If you change this, Windows domain authentication is disabled.

Installing the Steel-Belted Radius Server Software

To install the Steel-Belted Radius server software on a Windows server:

1. Log on to the Windows server as an administrator.
2. Make sure you have access to the downloaded Steel-Belted Radius Windows Installer Package either on the local system or via a network share.
   - Local installation – Copy the Steel-Belted Radius Windows Installer Package (Steel-Belted Radius.msi file) to your computer and run it locally.
   - Network installation – Locate and run the Steel-Belted Radius Windows Installer Package (Steel-Belted Radius.msi file) from a network server.
3. When the Welcome window opens, click **Next** to continue.

4. When the Customer Information window opens, enter your customer information.

   - Enter your user name in the **User Name** field.
   - Enter the name of your company in the **Organization** field.
   - If you are installing a purchased copy of the Steel-Belted Radius server, enter the license number printed on your license agreement card in the **Serial Number** field.
   - If you are installing an evaluation copy of the Steel-Belted Radius server, leave the **Serial Number** field blank and check the **Install 30-day trial** checkbox.

   Click **Next** to continue.

5. If you checked the **Install 30-day trial** checkbox in 4., use the Select Server Type window to specify which edition of the Steel-Belted Radius server software you want to install.

   The Steel-Belted Radius server software is available in three editions:

   - Global Enterprise Edition (GEE)
   - Service Provider Edition (SPE)
   - Enterprise Edition (EE) (with optional LDAP Configuration Interface support)

   Click **Next** to continue.

6. When the License Agreement window opens, read the agreement, click the **I accept the terms in the license agreement** radio button, and click **Next** to continue.

7. When the Custom Setup window appears, specify whether you want to change the default settings for installing Steel-Belted Radius.

   By default, the Steel-Belted Radius software and documentation is installed in the C:\Program Files\Juniper Networks\Steel-Belted Radius\Service directory. If you want to install the Steel-Belted Radius server software to a directory other than the default, click the **Change** button and specify your custom installation settings.

   Click **Next** to continue.

   If you are updating an existing Steel-Belted Radius installation, a window identifies the location where your current files will be archived. Click **Next** to continue.

8. When the Windows Account window opens, enter your Windows administrator account name in the **Account** field. Click **Next** to continue.

   The Windows account information you enter is the default login account for SBR Administrator. You must use this account name the first time you log into SBR Administrator.

NOTE: Make sure the login account you specify has a password. If a user without a password is specified as the administrator, the user will not be able to log into the SBR Administrator application.

9. When the Select Server Edition window opens, specify whether you want to install a standalone server, a primary server, or a replica server.

   - If you click the **Install as Standalone SBR Server** button, you do not need to specify replication information.
   - If you click the **Install as Primary SBR Server** button and click **Next**, you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter the replication secret in the **Primary Server Secret** and **Re-enter Secret** fields and click **Next** to continue.
   - If you click the **Install as Replica SBR Server** button and click **Next**, you are prompted to specify how the replica server can locate the replica package containing your Steel-Belted Radius replication settings.
     - If you want to browse for a replication package on your computer or network, click the **Browse for replica package** button, click the **Browse** button, and navigate to the directory containing the replica.ccmpkg file.
     - If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), click the **Provide Primary Server data** button, and specify the name, IP address(es), and replication secret of the primary server.

   Click **Next** to continue.

10. When the Start Services window opens, check the **Yes, start the Steel-Belted Radius service** checkbox if you want the Steel-Belted Radius service to start immediately. Click **Next** to continue.

11. If you want to register the Steel-Belted Radius server as an Agent Host with an RSA SecurID server, check the **Yes, I'd like to register** checkbox, click the **Browse** button, and navigate to the directory containing the sdconf.rec, radius.cer, server.cer, server.key, and failover.dat files.

NOTE: When you register your Steel-Belted Radius master or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

12. When the Ready to Install window opens, click **Install** to begin the installation.

    As the installation proceeds, the Installation Status window displays your progress.

13. When the Setup Complete window opens, check the **Show the readme file** checkbox if you want to review the release notes for the Steel-Belted Radius server software.

    Click **Finish**.

You must now finish configuring the new Steel-Belted Radius server to suit your network's authentication and accounting needs. For example, you can edit the [Addresses] section of the radius.ini file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the RADIUS service. Refer to "Starting the Steel-Belted Radius Service" on page 24 for information on starting the RADIUS service. Refer to the *Steel-Belted Radius Administration Guide* for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

NOTE: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the Administrator has a secure configuration environment and direct access to certificates.

Upgrading from a 30-Day Trial Installation

You can download an evaluation version of Steel-Belted Radius from the Juniper Networks website. If you want to continue using the product at the end of the 30-day evaluation period, you do not need to re-install the software. You can add a license number to your existing installation to convert it from evaluation mode to licensed mode.

1. Purchase the Steel-Belted Radius software by contacting your preferred reseller or by contacting Juniper Networks. You will be shipped a product package that contains a license number.

2. Start the SBR Administrator program and connect to your Steel-Belted Radius server.

3. Choose **File > License**.

4. When the Add a License for Server window opens, enter your license number and click **OK**.

   After you have entered a valid license number, the server displays a confirmation message and reminds you that you must restart the server.

5. Click **OK** to close the confirmation window.

6. Restart your Steel-Belted Radius server.

   The server does not restart itself automatically after a new license number is added. You must restart Steel-Belted Radius manually to activate the new license number.

7. Refer to the *Steel-Belted Radius Administration Guide* for information on using SBR Administrator.

Upgrading from Steel-Belted Radius Version 6.0 or 5.4

NOTE: Steel-Belted Radius v6.1 supports upgrades from v6.0 or v5.4. If you have an SBR installation earlier than v5.4, you must first upgrade to v6.0 or v5.4 before you attempt to move to v6.1.

NOTE: Do not uninstall your existing version of SBR before upgrading to v6.1.

NOTE: When you upgrade from Steel-Belted Radius v5.4, the v5.4 Administrator is not uninstalled. It remains on the system, but it is no longer functional. It is recommended that you manually uninstall the old Administrator using the procedure detailed in "Uninstall the SBR Version 5.4 Administrator" on page 23. While you should not uninstall the SBR server before upgrading, you can uninstall the SBR Administrator at any time.

Upgrading Steel-Belted Radius requires that you back up your Steel-Belted Radius files, install the new Steel-Belted Radius server software, and then merge your old configuration files (*.ini, *.aut, *.dir, *.pro, *.rr, *.eap) with the new configuration files.

Perform the following steps to upgrade your Steel-Belted Radius software from version 6.0 or 5.4 to version 6.1:

1. Export your Steel-Belted Radius database to an Extensible Markup Language (.xml) file.

   Refer to the *Steel-Belted Radius Administration Guide* for information on how to export your Steel-Belted Radius database to a .xml file.

2. Back up your *radiusdir* directory and the exported .xml file to an archive location.

   The Steel-Belted Radius installer backs up your files and database when it runs. The file archive created in this step ensures that your configuration is preserved in the event the installer fails before it finishes running.

3. Verify that you have your Steel-Belted Radius version 6.1 license number.

4. Close all applications running on your Steel-Belted Radius server.

   You do not need to stop the Steel-Belted Radius service when you upgrade the Steel-Belted Radius server software.

5. Start the installation for Steel-Belted Radius version 6.1 server software on your server.

   When the installation program detects the presence of a previous version of SBR installed on the system, you are prompted with information detailing what must happen next as part of the upgrade. The "Previous Install Detected" prompt says the following:

   > "Steel-Belted Radius version 6.1 uses a different database software program than was used by previous SBR releases. Therefore, if you want to preserve and use your current database configuration with the v6.1 release, as part of the product upgrade, the v6.1 installation must perform a data migration."

NOTE: If you choose not to perform the data migration (if you uncheck the **Migrate existing configuration database** checkbox presented to you in the "Convert the SBR Database" install window), your current database configuration will NOT be available to you in v6.1. In this case, if you uncheck the checkbox and click **Next**, you are informed that an empty configuration database will be created during the install.

   If the upgrade program attempt to migrate your existing database fails for some reason, you are prompted that the migration failed. The installation program aborts and you are told the check the DBConvert.log file, located in the service directory.

   Also, as part of the v6.1 upgrade process, after you enter all required configuration settings as part of the installation, the v6.1 upgrade program must then uninstall the previous SBR version. You are warned several times throughout the upgrade that the previous version will be uninstalled at the end of the upgrade process.

   After the database migration prompts, the following install prompts are standard license acceptance, directory selection, and administrator configuration setting prompts.

6. When the Select Server Edition window appears, specify whether you want to install a standalone server, a primary server, or a replica server.

   - If you click the **Install as Standalone SBR Server** button, you do not need to specify replication information.
   - If you click the **Install as Primary SBR Server** button and click **Next**, you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter the replication secret in the **Primary Server Secret** and **Re-enter Secret** fields and click **Next** to continue.

- If you click the **Install as Replica SBR Server** button and click **Next**, you are prompted to specify how the replica server can locate the replica package containing your Steel-Belted Radius replication settings.
  - If you want to browse for a replication package on your computer or network, click the **Browse for replica package** button, click the **Browse** button, and navigate to the directory containing the replica.ccmpkg file.
  - If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), click the **Provide Primary Server data** button, and specify the name, IP address(es), and replication secret of the primary server.

Click **Next** to continue.

7. When the Start Services window in the installer opens, uncheck the **Yes, start the Steel-Belted Radius service** checkbox to indicate you do not want the Steel-Belted Radius service to start. Click **Next** to continue.

   After the Steel-Belted Radius installer finishes running, the configuration and dictionary files that were in \Radius\Service are backed up in a new C:\Program Files\Juniper Networks\Steel-Belted Radius\Service_*Date_IDnumber* directory.

   For more information, see "Installing the Steel-Belted Radius Server Software" on page 15.

8. When you've finished entering the necessary configuration settings, the upgrade program is ready to proceed with the installation. You are presented with the "Ready to Install the Program" prompt. Here you are again warned that the previous installation will be uninstalled as part of the upgrade. Click the **Install** button to proceed.

NOTE: Do not cancel the Steel-Belted Radius installer after you start running it. Doing so may result in a loss of data.

9. When the v6.1 installation is complete, it starts the uninstall process for the previous version. You must click the **Yes** button when the "Are you sure you want to uninstall this product?" pop-up window appears. If you click the **No** button, you are cancelling the v6.1 upgrade and nothing you have configured is instantiated.

NOTE: The Steel-Belted Radius v6.1 upgrade must uninstall the previous version in order to complete successfully.

   When you start the uninstall program for the previous version, you are asked if you would like to save all user and\or application created files from the previous version.

10. When the v6.1 upgrade is complete and the "InstallShield Wizard Completed" window appears, click the **Finish** button.

11. Export your Steel-Belted Radius (version 6.1) database to an Extensible Markup Language (.xml) file.

    This step ensures that you have a clean copy of the Steel-Belted Radius database files (version 6.1) in the event you need them.

    Refer to the *Steel-Belted Radius Administration Guide* for information on how to export your Steel-Belted Radius database to an .xml file.

12. Back up your *radiusdir* directory and the exported .xml file to an archive location.

    This step ensures that you have a clean copy of the Steel-Belted Radius configuration files (version 6.1) in the event you need them.

13. Copy your backed-up configuration files (*.ini, *.aut, *.dir, *.pro, *.rr, *.eap) to C:\Program Files\Juniper Networks\Steel-Belted Radius\Service or merge the settings from your backed-up configuration files into the new Steel-Belted Radius configuration files.

    The configuration files installed as part of Steel-Belted Radius version 6.1 include settings that were not present in earlier versions.

    - If you want to preserve your previous settings (and if you want to use the default values for settings introduced in version 6.1 of Steel-Belted Radius), you can copy your archived configuration files to C:\Program Files\Juniper Networks\Steel-Belted Radius\Service, replacing the newly installed versions of those files.

    - If you want to use non-default settings for features of Steel-Belted Radius, you must merge the settings from your archived configuration files with the settings in the new configuration files.

NOTE: Do not merge the settings from the archived version of the eap.ini file to the newly installed default eap.ini file. Use SBR Administrator to apply the EAP settings you were using before the upgrade.

    Refer to the *Steel-Belted Radius Reference Guide* for information on the settings contained in each configuration file.

14. If you added your own dictionaries or modified the default Steel-Belted Radius dictionaries, re-add your custom dictionaries or modify the dictionaries installed with the Steel-Belted Radius version 6.0 software as appropriate.

15. Restart the Steel-Belted Radius service.

    Choose **Start > Control Panel > Administrative Tools > Services**. Choose the **Steel-Belted Radius** entry. Click **Restart the service**.

16. Run SBR Administrator and verify that your configuration settings are complete and correct.

NOTE: It is recommended that you run the SBR Administrator application locally when configuring the server. This way, the SBR Administrator has a secure configuration environment and direct access to certificates.

Uninstall the SBR Version 5.4 Administrator

When you upgrade from Steel-Belted Radius v5.4, the v5.4 SBR Administrator is not uninstalled. It remains on the system, but it is no longer functional. You should manually uninstall the old SBR Administrator using the following procedure.

1. Choose **Start > Control Panel > Add or Remove Programs**.
2. When the Add or Remove Programs control panel opens, select the **Steel-Belted Radius Administrator** for V5.4. (You may have multiple Steel-Belted Administrator programs listed. Note that the older Administrator uses the old Funk icon to distinguish it. Make sure you uninstall the older version and not the newly installed version of the Administrator.)
3. Click **Remove**.
4. When a window asking you to confirm you want to remove Steel-Belted Radius Administrator opens, click **Yes**.
5. After the control panel indicates the SBR Administrator software has been uninstalled, archive or delete files remaining in the \Radius\Admin directory.

Restoring a Previous Configuration

When you install the Steel-Belted Radius server software, the installation script saves your existing configuration to a backup directory to preserve your configuration settings. If you are re-installing the same version and edition of Steel-Belted Radius on a server, you can copy the configuration files from the backup directory to the Steel-Belted Radius server directory to restore your previous configuration.

If you are upgrading your Steel-Belted Radius software from an older version, do not copy your configuration files to the Steel-Belted Radius server directory. For more information, see “Upgrading from Steel-Belted Radius Version 6.0 or 5.4” on page 19.

Stopping the Steel-Belted Radius Service

After the Steel-Belted Radius service is installed on a Windows server, it stops and starts automatically each time you shut down or restart the server. You can stop the Steel-Belted Radius service at any time by performing the following steps:

1. Choose **Start > Control Panel > Administrative Tools > Services**.
2. When the Services window opens, click the **Steel-Belted Radius** entry.
3. Click the **Stop the service** button.

Starting the Steel-Belted Radius Service

You must restart the Steel-Belted Radius service after you modify configuration files. To start the Steel-Belted Radius server after it has been stopped:

1. Choose **Start > Control Panel > Administrative Tools > Services**.
2. When the Services window opens, click the **Steel-Belted Radius** entry.
3. Click the **Start the service** button.

To restart the Steel-Belted Radius server without stopping it:

1. Choose **Start > Control Panel > Administrative Tools > Services**.
2. When the Services window opens, click the **Steel-Belted Radius** entry.
3. Click the **Restart the service** button.

Chapter 4

Solaris Installation

This chapter describes how to install or upgrade the Steel-Belted Radius server software on a Solaris server. This chapter also describes how to install the optional SNMP software for use with the GEE and SPE editions of Steel-Belted Radius.

Before You Begin

- Verify that the proposed installation host complies with the hardware and software requirements of Steel-Belted Radius. For more information, see "System Requirements – Solaris" on page 10.
- Make sure that you are (or have access to) a system administrator and someone who understands your RADIUS authentication and accounting requirements.
- If you are installing the optional SNMP module, stop all SNMP agents running on your server.

NOTE: If your server runs SNMP agents other than the one supplied with Steel-Belted Radius, you must coordinate the port numbers used by your SNMP agents to avoid port contention.

Upgrade Files

The install, configure, and uninstall scripts for Steel-Belted Radius version 6.1 automatically archive your Steel-Belted Radius files to the /radius/install/backups directory. To facilitate future software upgrades, the install, configure, and uninstall scripts create a number of .dat files in the /radius/install directory. These files store information used for future upgrades. You should not move, rename, or otherwise modify these files.

Table 6: Upgrade Files and Directories

File	Function
radius/install/package.dat	Contains a unique package identifier.
radius/install/preinstall.dat	Contains the absolute pathname of the backup directory for your old Steel-Belted Radius software and configuration files (pre-installation backup).
radius/install/install.dat	Contains the absolute pathname of the backup directory for your Steel-Belted Radius v6.1 software and configuration files, as shipped without modification (post-installation backup).
radius/install/upgrade.dat	Contains the absolute pathname of the Steel-Belted Radius version 6.1 upgrade source (if any).
radius/install/configure.dat	Contains configuration state data.
radius/install/uninstall.dat	Contains the absolute pathname of the backup directory for your Steel-Belted Radius v6.1 software and working configuration files (pre-uninstall backup).
radius/install/backups/	Contains the backups referenced by the.dat files.

Package Management Commands

Table 7 lists useful Solaris package management commands.

Table 7: Useful Package Management Commands

Command	Function
pkginfo -x |egrep "FUNK|JNPR|RSAR"	Report any pre-existing packages and patches.
pkginfo -l JNPRsbrge	Report high level description for specified package
pkginfo -r JNPRsbrge	Show installed directory
pkgadd -d /path/to/JNPRsbrge.sol.pkg [-a none] JNPRsbrge.sol.pkg	Install [at specified */path*]
pkgrm JNPRsbrge	Uninstall Steel-Belted Radius.

Installing the Steel-Belted Radius Server Software

The installer for the Solaris version of the Steel-Belted Radius server software uses pkgadd files, which have filenames that include the edition and version of the server software

NOTE: This section assumes that you are installing Steel-Belted Radius on your Solaris server for the first time or that you are installing Steel-Belted Radius in a directory other than the one used by previous installations (clean installation). If you are upgrading an existing Steel-Belted Radius installation to version 6.1, refer to "Upgrading from Steel-Belted Radius Versions 6.0 or 5.4" on page 34 for information on upgrade options and considerations.

To install the Steel-Belted Radius server software on a Solaris server:

1. Log into the Solaris server as root.

2. Copy the downloaded Steel-Belted Radius installation files to the Solaris server. Make sure to copy them to a local or remote hard disk partition that is readable by root. The following example copies the files to the /opt/JNPRsbr/temp directory.

   ```
   # mkdir -p /opt/JNPRsbr/temp
   # cp -pR /cdrom/sbr/solaris/* /opt/JNPRsbr/temp
   ```

3. Uncompress the Steel-Belted Radius installation package.

   ```
   # gunzip -dc JNPRsbrXX.sol.pkg.tgz |tar xf -
   ```

   where *XX* specifies the version of Steel-Belted Radius you want to install:

   - ge – Steel-Belted Radius/Global Enterprise Edition (JNPRsbrge)
   - sp – Steel-Belted Radius/Service Provider Edition (JNPRsbrsp)
   - ee – Steel-Belted Radius/Enterprise Edition (JNPRsbree)

4. Run the installer package.

   ```
   # pkgadd -d directory -a none JNPRsbrXX.sol.pkg
   ```

   where *directory* specifies the directory where you placed the installation package and *XX* specifies the version of Steel-Belted Radius you want to install.

   ```
   # pkgadd -d /export/home/carter/sbr -a none JNPRsbrge.sol.pkg

   Processing package instance <JNPRsbrge.sol.pkg> from
       </export/home/carter/sbr>

   JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition)
   (sparc) 6.1.0000
   (C) Copyright 1996-2007 Juniper Networks, Inc. See license.txt
   ```

5. Specify the base directory in which you want to install the Steel-Belted Radius files.

   By default, the installation package puts the Steel-Belted Radius files in the /opt/JNPRsbr/ base directory.

   ```
   Enter path to package base directory [?,q] /opt/JNPRsbr

   The selected base directory </opt/JNPRsbr> must exist before installation is
       attempted.
   Do you want this directory created now [y,n,?,q] y
   Using </opt/JNPRsbr> as the package base directory.
   ## Processing package information.
   ## Processing system information.
   ## Verifying disk space requirements.
   ## Checking for conflicts with packages already installed.
   ## Checking for setuid/setgid programs.
   ```

6. When you are prompted to confirm you want to install the package, enter **y**.

   ```
   This package contains scripts which will be executed with super-user
       permission during the process of installing this package.
   Do you want to continue with the installation of <JNPRsbrge> [y,n,?] y

   Installing JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise
       Edition) as <JNPRsbrge>

   ## Executing preinstall script.
   ## Installing part 1 of 1.
   ⋮
   ## Executing postinstall script.

   Newly installed server directory will be backed up as:
   /opt/JNPRsbr/radius/install/backups/2006:12:15-06:39:56
   Installation of <JNPRsbrge> was successful.
   ```

7. Navigate to the directory where you installed Steel-Belted Radius.

   ```
   # cd /opt/JNPRsbr/radius/install
   ```

8. Execute the following command to run the configuration script for the Steel-Belted Radius server software:

   ```
   # ./configure
   ```

9. Review the Steel-Belted Radius license agreement.

   Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter **y**.

   ```
   Do you accept the terms in the license agreement? [n] y
   ```

10. Indicate whether you have a license for your Steel-Belted Radius software.

    ```
    You can enter a license string or use a one-time 30 day trial license.
    Would you like to enter a license string? [n]
    ```

```
Installed a 30 day evaluation license.
```

- If you purchased Steel-Belted Radius, type **y** and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

- If you do not have a license number, type **n** and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product's full feature set for a limited period.

11. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI).

```
Do you wish to enable LCI? [n]
License does not have LCI support.
```

12. Specify whether you are upgrading an existing Steel-Belted Radius installation or configuring a new installation.

    - Enter n if you are performing a new installation.

    - Enter the directory path to the Steel-Belted Radius files if you are upgrading an existing Steel-Belted Radius installation and you know the name of the current Steel-Belted Radius directory.

    - Enter s if you are upgrading an existing Steel-Belted Radius installation and you want to search for the Steel-Belted Radius directory.

```
Please enter backup or radius directory from which to upgrade.
Enter n for new configuration, s to search, or q to quit.
[n] n
```

13. Specify that you do not want to remove older versions of Steel-Belted Radius.

```
WARNING: Now is the best time to remove any pre-existing versions of the
    software, as doing so later may destroy certain shared OS resources,
    such as /etc/init.d scripts in particular, that are about to be configured.
    Obsolete patches may also be removed.
Manually remove pre-existing software now? [y]: n
```

14. Specify the login name of the initial Steel-Belted Radius administrator.

    The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

```
Enter initial admin user (account must have an associated password) [root]:
```

NOTE: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

15. Specify whether you want to install the Steel-Belted Radius server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

    Configure SBR server as primary (p), replica (r), or stand alone (sa) [sa]: **sa**

    - If you enter p (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.

      If appropriate, enter **y** when you are asked whether you are upgrading a primary server. Doing so tells the installer to preserve the server's replication realm information.

    - If you enter r (replica server), you are prompted to specify how the replica server can locate the replica.ccmpkg configuration package containing your Steel-Belted Radius replication settings.

      - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.

      - If you want to specify the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address, and replication secret of the primary server.

      If appropriate, enter **y** when you are asked whether you are upgrading a replica server. Doing so tells the installer to preserve the replica server's replication settings.

    - If you enter sa (standalone RADIUS server), you do not need to specify replication information.

16. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

    - If you do not want to configure Steel-Belted Radius for use with an external LDAP data service, press Enter.

    - If you want to configure Steel-Belted Radius for use with an external LDAP data service, type **y** and press Enter. You are prompted to enter the path for the LDAP library files:

      Do you want to configure LDAP? [n]: **y**
      Enter path for LDAP library files [/usr/lib]:

    To accept the default path (/usr/lib), press Enter.

17. Specify whether you want to configure Steel-Belted Radius for use with an Oracle database.

    Configuring for use with generic database
    Do you want to configure for use with Oracle? [n]:

    If no, press Enter.

If yes, type **y** and press Enter. You are prompted to version and path information for the Oracle library files.

```
Configuring for use with Oracle.
Supported Oracle version: 9, 10
What version of Oracle will be used? [9] 10
Configuring for use with Oracle 10
Setting the environment variable ORACLE_HOME.
Enter ORACLE_HOME []: /opt/10g/app/oracle/product/10.2.0.3
Setting the environment variable LD_LIBRARY PATH.
Enter path for Oracle shared libraries
    [/opt/10g/app/oracle/product/10.2.0.3/lib32]:
Setting the environment variable TNS_ADMIN.
Enter TNS_ADMIN [/opt/10g/app/oracle/product/10.2.0.3/network/admin]:
```

NOTE: Steel-Belted Radius requires that you use the Oracle 10 32-bit executables, which are stored in the /lib32 directory. Steel-Belted Radius is not compatible with the Oracle 10 64-bit executables stored in the /lib directory.

18. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can to monitor your Steel-Belted Radius server from an SNMP management station.

    ```
    Do you want to configure SNMP? [n]:
    ```

    If no, press Enter to proceed to the next prompt.

    If yes, type **Y** and press Enter. The installer prompts you for the information it needs to configure the funksnmpd.conf and startsnmp.sh files.

    a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

       ```
       Choose a community string: public
       ```

    b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing format. To specify that only one host may query the agent, enter the IP address of the host followed by /32. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

       ```
       Specify the range of IPv4 addresses that may query this agent, such as
           1.2.3.0/24.
       Address range: 192.168.70.0/24
       ```

    c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the SNMP subagent on the Steel-Belted Radius server.

       ```
       SNMPv2 trap sink: 192.168.70.86
       Configuration of SNMP complete.
       ```

NOTE: Refer to the *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

19. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

    ```
    Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1
        or later)? [n]:
    ```

NOTE: When you register your Steel-Belted Radius master or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

20. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

    ```
    Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: e
    ```

    Steel-Belted Radius stores its autoboot settings in the local *radiusdir*\radius\sbrd file.

    - If you enter **e** (enable), the configure script copies the settings in the **sbrd** file to the **/etc/init.d** boot script and deletes old Steel-Belted Radius autoboot settings, thereby enabling autobooting for Steel-Belted Radius v6.1.
    - If you enter **d** (disable), the configure script does not copy the settings in the **sbrd** file to the **/etc/init.d** boot script and deletes old Steel-Belted Radius autoboot settings, thereby disabling autobooting for all versions of Steel-Belted Radius.
    - If you enter **p** (preserve), the configure script does not copy the settings in the **sbrd** file to the **/etc/init.d** boot script or delete old Steel-Belted Radius autoboot settings, thereby leaving your previous autoboot settings unchanged.

Next Steps

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

```
The SBR Administrator can be launched using the following URL:
http://<servername>:1812
Configuration complete
```

You must now finish configuring the new Steel-Belted Radius server to suit your network's authentication and accounting needs. For example, you can edit the [Addresses] section of the **radius.ini** file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the RADIUS process. Refer to "Starting the RADIUS Server" on page 49 for information on starting the RADIUS process. Refer to the *Steel-Belted Radius Administration Guide* for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

NOTE: When you copy a license to the system, all features may not be available until you restart the SBR Administrator. After installing a license, the SBR Administrator should be restarted, as well as the server.

NOTE: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the SBR Administrator has a secure configuration environment and direct access to certificates.

Upgrading from a 30-Day Trial Installation

You can download an evaluation version of Steel-Belted Radius from the Juniper Networks website (http://www.juniper.net/products_and_services/). If you want to continue using the product at the end of the 30-day evaluation period, you do not need to re-install the software. You can add a license number to your existing installation to convert it from evaluation mode to licensed mode.

1. Purchase the Steel-Belted Radius software by contacting your preferred reseller or by contacting Juniper Networks. You will be shipped a product package that contains a license number.

2. Start the SBR Administrator and connect to your Steel-Belted Radius server.

   Refer to the *Steel-Belted Radius Administration Guide* for information on using the SBR Administrator.

3. Choose **File > License**.

4. When the Add a License for Server window opens, enter your license number and click **OK**.

   After you have entered a valid license number, the server displays a confirmation message and reminds you that you must restart the server.

5. Click **OK** to close the confirmation window.

6. Restart your Steel-Belted Radius server.

The server does not restart itself automatically after a new license number is added. You must restart Steel-Belted Radius manually to activate the new license number. Refer to "Starting the RADIUS Server" on page 49 for information on how to restart your Steel-Belted Radius server.

Upgrading from Steel-Belted Radius Versions 6.0 or 5.4

NOTE: Steel-Belted Radius v6.1 only supports upgrades from v6.0 or v5.4. If you have an SBR installation earlier than v5.4, you must first upgrade to v6.0 or v5.4 before you attempt to move to v6.1.

The procedure for upgrading your Steel-Belted Radius software has changed from previous (5.x) releases. Previously, you backed up and uninstalled your old Steel-Belted Radius software before installing new software. Steel-Belted Radius version 6.1 allows you to install your new software before deleting your old software. Steel-Belted Radius version 6.1 also helps you migrate your configuration and data files during the upgrade process.

Before You Begin

Before you upgrade your Steel-Belted Radius software from versions 5.4 or 6.0 to version 6.1 on a server, you should answer the following questions:

Do you want to relocate your Steel-Belted Radius files?

By default, Steel-Belted Radius v6.1 installs in the opt/JNPRsbr directory. You do not have to use the default installation directory.

When upgrading, note that the default installation directory for Steel-Belted Radius v5.4 software is /opt/funk directory. The default installation directory for Steel-Belted Radius v6.0 is /opt/JNPRsbr.

Do you want to retain your current Steel-Belted Radius configuration settings?

When you upgrade your Steel-Belted Radius software to version 6.1, you can start with the default Steel-Belted Radius configuration files, or you can choose to retain your current configuration files (data migration). The Steel-Belted Radius installer can create the following backups:

- Pre-installation backup—If you install Steel-Belted Radius v6.1 over a 6.0 or 5.4 version, the installer copies your old software and configuration settings to a backup directory (*basedir*/radius/install/backups/*YYYY:MM:DD:HH:MM:SS*). The name of this pre-installation backup is recorded in the preinstall.dat file (described on page 26). The installer displays a message identifying the name of the pre-installation backup ("Existing server directory will be backed up as....")

- Post-installation backup—The installer always copies the default Steel-Belted Radius version 6.1 software and configuration settings to a backup directory (*basedir*/radius/install/backups/*YYYY:MM:DD:HH:MM:SS*). The name of this post-installation backup is recorded in the install.dat file (described on page 26). The installer displays a message identifying the name of the post-installation backup ("Newly installed server directory will be backed up as....")

If you want to preserve your previous configuration settings, you can tell the configure script to migrate your settings from the pre-installation directory (or from another backup directory) to the working (/radius) directory. You would then copy parameters from the default configuration files in the post-installation backup to your configuration files to set up new Steel-Belted Radius features.

If you want to start with the default Steel-Belted Radius v6.1 settings, you can tell the configure script to skip the data migration and install the default configuration files. You could then merge settings from the archive files in the pre-installation backup directory to the default files to re-create your current configuration.

NOTE: Do not modify the backup directories or the .dat files that identify them. If you do, you may have difficulty upgrading your Steel-Belted Radius software in the future.

If you specify that you want to retain your current Steel-Belted Radius configuration settings when you run the installation script, the installer puts the default Steel-Belted Radius version 6.1 configuration files in the */radiusdir*/install directory.

Do you want to retain your old Steel-Belted Radius software?

During the configuration process, you will be asked whether you want to uninstall your old Steel-Belted Radius software. If you indicate that you do, the configure script will terminate so you can uninstall your old software manually. After you have uninstalled your old Steel-Belted Radius software, you can restart the configuration script to resume the installation/configuration process.

Figure 1 presents a decision tree that summarizes the choices you make and tasks you perform when upgrading from Steel-Belted Radius v6.0 or v5.4 to Steel-Belted Radius v6.1.

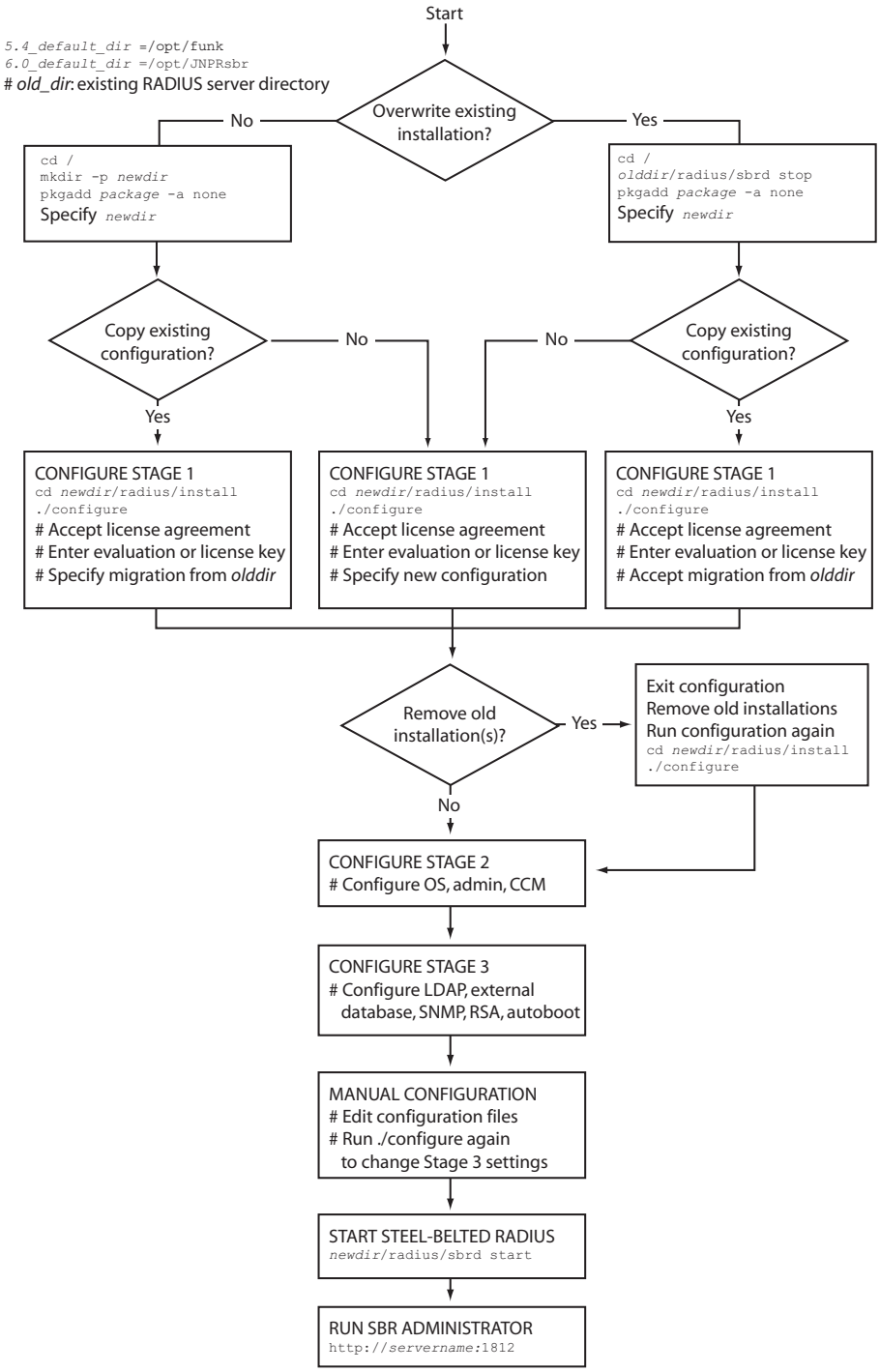
The configuration process consists of three phases. Note the following:

- In Stage 1, you specify whether you want to use your current data files to configure Steel-Belted Radius (data migration). After Stage 1 is complete, you will be asked whether you want to delete your old Steel-Belted Radius software.

- In Stage 2, you specify a default administrator and a centralized configuration management (CCM) role (stand-alone, primary server, or replica server).

- In Stage 3, you specify configuration information for LDAP, external databases, SNMP, autoboot (sbrd script), and whether you want your server to function as an Agent Host with RSA Authentication Manager. If you re-run the configure script in the future, it will automatically start at Stage 3.

Figure 1: Decision Tree for Steel-Belted Radius Upgrades (Solaris version)



The following scenarios apply to upgrading from v5.4 to v6.1 as follows:

- Scenario 1 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/funk directory) that retains the existing configuration information. The old software is archived and overwritten with the new software. The default version 6.1 configuration files are copied to the /opt/funk/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 2 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the software in the old /opt/funk directory is preserved) that retains the existing configuration information. The default version 6.1 configuration files are copied to the /opt/JNPRsbr/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 3 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that retains the existing configuration information. The default version 6.1 configuration files are copied to the /opt/JNPRsbr/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 4 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/funk directory) that installs clean (default) version 6.1 configuration files. The old software and configuration settings are archived in the /opt/funk/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use your archived configuration files to merge customized settings into your new configuration files manually.

- Scenario 5 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the software in the old /opt/funk directory is preserved) that installs clean (default) version 6.1 configuration files. You can merge customized settings from your old configuration files into your new configuration files manually. This scenario would be appropriate in situations where you want to install and experiment with a new release of Steel-Belted Radius before discarding older releases.

- Scenario 6 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that installs clean (default) version 6.1 configuration files. If you archived your old settings manually, you can use your archived configuration files to merge customized settings into your new configuration files.

The following scenarios apply to upgrading from v6.0 to v6.1 as follows:

- Scenario 1 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/JNPRsbr directory) that retains the existing configuration information. The old software is archived and overwritten with the new software. The default version 6.1 configuration files are copied to the /opt/JNPRsbr /radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 2 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is not installed in the default directory, but in a directory of your choosing, and the old /opt/JNPRsbr directory and the software in the old /opt/JNPRsbr directory are both preserved) that retains the existing configuration information. The default version 6.1 configuration files are copied to the newdir/radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 3 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in a directory of your choosing and the old /opt/JNPRsbr directory is deleted) that retains the existing configuration information. The default version 6.1 configuration files are copied to the newdir/radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use these files to merge new settings into your configuration files manually.

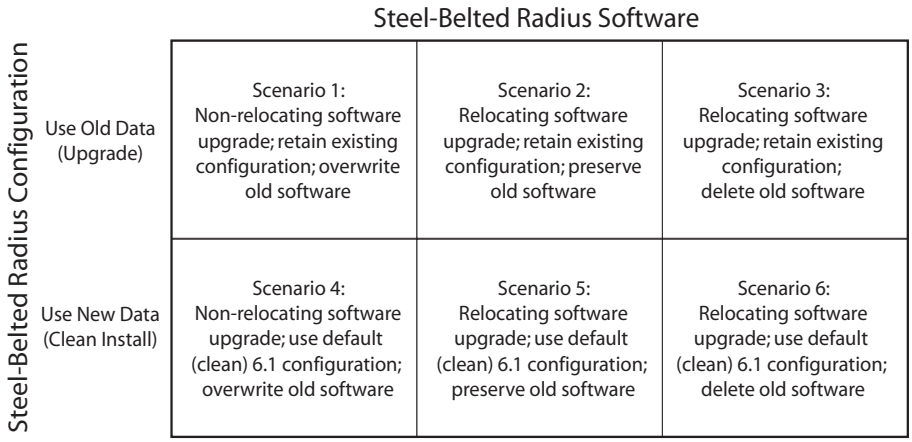
- Scenario 4 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/JNPRsbr directory) that installs clean (default) version 6.1 configuration files. The old software and configuration settings are archived in the /opt/JNPRsbr/radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use your archived configuration files to merge customized settings into your new configuration files manually.

- Scenario 5 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is installed in a directory of your choosing and the /opt/JNPRsbr directory and the software in the old /opt/JNPRsbr directory are both preserved) that installs clean (default) version 6.1 configuration files. You can merge customized settings from your old configuration files into your new configuration files manually. This scenario would be appropriate in situations where you want to install and experiment with a new release of Steel-Belted Radius before discarding older releases.

- Scenario 6 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in a directory of your choosing and the old /opt/JNPRsbr directory is deleted) that installs clean (default) version 6.1 configuration files. If you archived your old settings manually, you can use your archived configuration files to merge customized settings into your new configuration files.

Figure 2 presents this decision process as a set of upgrade scenarios:

Figure 2: Upgrade Scenarios


Steel-Belted Radius Software
Steel-Belted Radius Configuration
Use Old Data (Upgrade)
Use New Data (Clean Install)
Scenario 1: Non-relocating software upgrade; retain existing configuration; overwrite old software
Scenario 2: Relocating software upgrade; retain existing configuration; preserve old software
Scenario 3: Relocating software upgrade; retain existing configuration; delete old software
Scenario 4: Non-relocating software upgrade; use default (clean) 6.1 configuration; overwrite old software
Scenario 5: Relocating software upgrade; use default (clean) 6.1 configuration; preserve old software
Scenario 6: Relocating software upgrade; use default (clean) 6.1 configuration; delete old software

Begin the Upgrade Procedure

Perform the following steps to upgrade your Steel-Belted Radius software from versions 6.0 or 5.4 to version 6.1 on a Solaris server.

NOTE: Do not uninstall your existing version of SBR before upgrading to v6.1.

1. Log into the Solaris server as root.

2. Back up your */radiusdir* directory to an archive location.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup. This backup directory is needed for data migration tasks that are associated with future upgrades.

   For v6.0:
   # cd /opt/JNPRsbr
   # mkdir /opt/backups
   # tar cf - radius | (cd /opt/backups; tar xfBp -)

   or

   For v5.4:
   # cd /opt/funk
   # mkdir /opt/backups
   # tar cf - radius | (cd /opt/backups; tar xfBp -)

3. Back up your root and server certificates, and verify you know the password for your server certificate.

   You will install your server certificate for Steel-Belted Radius v6.1 by running the SBR Administrator configuration application.

4. Stop the RADIUS process currently running on your server.

For v6.0:
 # /opt/JNPRsbr/radius/sbrd stop

or

For v5.4:
 # /opt/funk/radius/sbrd stop

5. If you installed the 969531-01 or 969541-01 security patch for Steel-Belted Radius v5.4, uninstall the security patch.

   You must uninstall the security patch manually, using the appropriate package removal command (pkgrm).

6. Copy the Steel-Belted Radius installation files to the Solaris server. Make sure to copy them to a local or remote hard disk partition that is readable by root. The following example copies the files to the /opt/JNPRsbr/temp directory.

   # cd /
   # mkdir -p /opt/JNPRsbr/temp
   # cp -pR /cdrom/sbr/solaris/* /opt/JNPRsbr/temp

7. Run the installer package.

   # pkgadd -d *directory* -a none JNPRsbr*XX*.sol.pkg

   where *directory* specifies the directory where you placed the installation package and *XX* specifies the version of Steel-Belted Radius you want to install.

   # pkgadd -d /opt/JNPRsbr/temp -a none JNPRsbrge.sol.pkg

   Processing package instance <JNPRsbrge.sol.pkg> from
   </opt/JNPRsbr/temp>

   JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition)
   (sparc) 6.1.0000
   (C) Copyright 1996-2007 Juniper Networks, Inc. See license.txt

8. You are asked if you want to create a new instance of the package. For upgrades, if you answer **y** here, the install path is unrestricted and you can install the package in any directory. If you answer **n** here, you are restricted to installing to the same directory in which the version you are upgrading is installed.

   Do you want to create a new instance of this package [y,n,?,q] **n**

   The following instance(s) of the <JNPRsbrge> package are
   already installed on this machine:
   1 JNPRsbrge JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition)
   (sparc) 6.0.0000

9. The installation next asks if you want to overwrite the current installation. For upgrades, you would answer yes.

   Do you want to overwrite this installed instance [y,n,?,q] **y**

10. Specify the base directory in which you want to install the Steel-Belted Radius files.

    Enter path to package base directory [?,q] **/opt/JNPRsbr**

    Using </opt/JNPRsbr> as the package base directory.
    ## Processing package information.
    ## Processing system information.
    ## Verifying disk space requirements.
    ## Checking for conflicts with packages already installed.
    ## Checking for setuid/setgid programs.

11. When you are prompted to confirm you want to install the package, enter **y**.

    This package contains scripts which will be executed with super-user permission during the process of installing this package.
    Do you want to continue with the installation of <JNPRsbrge> [y,n,?] **y**

    Installing JNPRsbrge - Juniper Networks Steel-Belted Radius (Global Enterprise Edition) as <JNPRsbrge>

    ## Executing preinstall script.
    ## Installing part 1 of 1.
    ⋮
    ## Executing postinstall script.

    Newly installed server directory will be backed up as:
    /opt/JNPRsbr/radius/install/backups/2006:12:15-06:39:56
    Installation of <JNPRsbrge> was successful.

12. Navigate to the directory where you installed Steel-Belted Radius.

    # **cd /opt/JNPRsbr/radius/install**

13. Navigate to the directory where you installed Steel-Belted Radius and run the configuration script for Steel-Belted Radius.

    # **cd /opt/JNPRsbr/radius/install**
    # **./configure**

14. Review the Steel-Belted Radius license agreement.

    Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter **y**.

    Do you accept the terms in the license agreement? [n] **y**

15. Indicate whether you have a license number.

    You can enter a license string or use a one-time 30 day trial license.
    Would you like to enter a license string? [n]

- If you purchased Steel-Belted Radius, type **y** and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

- If you do not have a license number, type **n** at the prompt and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product's full feature set for a limited period.

16. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI).

    Do you wish to enable LCI? [n]
    License does not have LCI support.
    Installed a 30 day evaluation license.

17. Specify whether you want to migrate your current Steel-Belted Radius configuration files.

    - If you are performing a non-relocating update (or if you are performing a relocating update and you want to migrate your configuration files), specify the directory path to your current Steel-Belted Radius files. If you are performing a non-relocating update, the default is the pre-installation backup of your current settings.

      Please enter backup or radius directory from which to upgrade.
      Enter n for new configuration, s to search, or q to quit.
      [/*radiusdir*/radius/install/backups/*timestamp*]

      Press Enter to accept the default value, or enter a different path if you want to use a different set of configuration files. You can enter **s** if you want to search for the directory path for your Steel-Belted Radius files.

    - If you are performing a relocating update (and you do not want to migrate your configuration files), enter **n** to specify that you want to use the default configuration files.

      Please enter backup or radius directory from which to upgrade.
      Enter n for new configuration, s to search, or q to quit.
      [n] **n**

18. Specify whether you want to remove your old Steel-Belted Radius software.

    If you want to remove your old Steel-Belted Radius software, enter **y** at the Manually remove pre-existing software now? prompt, uninstall the old software, and then run the configuration script again. When you restart the configuration script, the script returns you to this step.

    WARNING: Now is the best time to remove any pre-existing versions of the software, as doing so later may destroy certain shared OS resources, such as /etc/init.d scripts in particular, that are about to be configured. Obsolete patches may also be removed.
    Manually remove pre-existing software now? [y]: **y**
    Please execute configure again when you are finished

Administrator deletes old Steel-Belted Radius files:

Steel-Belted Radius version 6.0: **pkgrm JNPRsbr*XX***

Steel-Belted Radius version 5.4: **pkgrm FUNKsbr*XX***

Administrator then restarts the configure script:

```
# cd /opt/JNPRsbr/radius/install
# ./configure
```

19. Specify the login name of the initial Steel-Belted Radius administrator.

    The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

    Enter initial admin user (account must have an associated password) [root]:

NOTE: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

20. If you are not migrating your old configuration data (that is, if you answered n in Step 15, specify whether you want to install the Steel-Belted Radius server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

    Configure SBR server as primary (p), replica (r), or stand alone (sa) [sa]: **r**

    - If you enter p (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.
    - If you enter r (replica server), you are prompted to specify how the replica server can locate the replica package containing your Steel-Belted Radius replication settings.
        - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.
        - If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address(es), and replication secret of the primary server.
    - If you enter sa (standalone RADIUS server), you do not need to specify replication information.

21. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

    Do you want to configure LDAP? [n]:
    - If no, press Enter.

- If yes, type **y** and press Enter. You are prompted to enter the path for the LDAP library files:

```
Enter path for LDAP library files [/usr/lib]:
```

To accept the default path (/usr/lib), press Enter.

22. Specify whether you want to configure Steel-Belted Radius for use with an Oracle database.

```
Configuring for use with generic database
Do you want to configure for use with Oracle? [n]:
```

If no, press Enter.

If yes, type **y** and press Enter. You are prompted to version and path information for the Oracle library files.

```
Configuring for use with Oracle.
Supported Oracle version: 9, 10
What version of Oracle will be used? [9] 9
Configuring for use with Oracle 9
Setting the environment variable ORACLE_HOME.
Enter ORACLE_HOME []: /opt/10g/app/oracle/product/9.2.0
Setting the environment variable LD_LIBRARY PATH.
Enter path for Oracle shared libraries:
    /opt/10g/app/oracle/product/9.2.0/lib
Setting the environment variable TNS_ADMIN.
Enter TNS_ADMIN: /opt/10g/app/oracle/product/9.2.0/network/admin
```

23. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can to monitor your Steel-Belted Radius server from an SNMP management station.

```
Do you want to configure SNMP? [n]:
```

If no, press Enter to proceed to the next prompt.

If yes, type **y** and press Enter. The configure script prompts you for the information it needs to configure the jnprsnmpd.conf and startsnmp.sh files.

a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

```
Choose a community string: public
```

b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing (CIDR) format. To specify that only one host may query the agent, enter the IP address of the host followed by /32. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

```
Specify the range of IPv4 addresses that may query this agent, such as
```

1.2.3.0/24.
Address range: **192.168.70.0/24**

c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the Steel-Belted Radius server.

SNMPv2 trap sink: **192.168.70.86**
Configuration of SNMP complete.

NOTE: Refer to the *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

24. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1 or later)? [n]:

NOTE: When you register your Steel-Belted Radius primary or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

25. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: **e**

- If you enter **e**, the configure script saves the **sbrd** script and copies it to the **/etc/init.d** boot script.
- If you enter **d**, the configure script discards changes made to the **sbrd** script.
- If you enter **p**, the configure script saves the **sbrd** script and but does not copy it to the **/etc/init.d** boot script.

Next Steps

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

The SBR Administrator can be launched using the following URL:
http://<servername>:1812
Configuration complete

You must now finish configuring the new Steel-Belted Radius server to suit your network's authentication and accounting needs. For example, you can edit the [Addresses] section of the **radius.ini** file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the radius process. Refer to "Stopping the RADIUS Server" on page 49 for information on starting the RADIUS process. Refer to the *Steel-Belted Radius Administration Guide* for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

NOTE: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the Administrator has a secure configuration environment and direct access to certificates.

Additional Required Manual File Upgrades

Upgrading from v6.0 or v5.4 to v.61 requires some additional, manual upgrading of certain configuration files. The files and file types listed in this section are those that require manual migration. All other files are automatically migrated during the upgrade process.

Manual Migration of XML configurations

You must manually migrate the following XML files by merging any changed values into the corresponding XML files that are shipped with the new Steel-Belted Radius software installation (you should never modify any other *.xml files):

- radius/sbr_administration.xml - socket port number specified by port = setting
- radius/sbr_ccm.xml - socket port numbers specified by port = settings
- radius/sbr_id.xml - hostname specified by id = setting
- system/config/logging_mgr.xml - logStream events = settings

The IP addresses, hostnames, socket port numbers, and other similar data entries found in these files often have corresponding parameters in the radius.ini file which must be kept in agreement.

Manual Migration of JRE Extensions

Steel-Belted Radius ships its own Java Runtime Environment (JRE) to facilitate JDBC plug-ins and Java Scripting. You can extend the JRE by installing third-party .jar files in the radius/jre/lib/ext subdirectory. You must migrate any third party .jar files by copying them to the new Steel-Belted Radius software installation.

Note that the following .jar files are shipped with Steel-Belted Radius and should not be migrated:

- dnsns.jar
- funk-sql.jar
- localedata.jar
- sunjce_provider.jar

- sunpkcs11.jar

Manual Migration of JavaScript files

As of v5.4, all JavaScript files (*.jsi) are stored in the radius/scripts subdirectory. Any JavaScript files must be migrated manually to v6.1 by copying them to the new Steel-Belted Radius software installation.

Manual Migration of ROOT Certificates

As of v5.4, the storage of root certificates is managed by the Steel-Belted Radius server and the SBR Administrator is used to add and delete root certificates. You must manually migrate root certificates by using the SBR Administrator to add them from the old root directory.

Manual Migration of SNMP Configuration

SNMP configuration is contained in the radius/snmp/conf directory (for example, radius/snmp/conf/jnprsnmpd.conf). You must manually migrate this configuration by merging the contents of the files into the files that are shipped with the new Steel-Belted Radius software installation. But if you choose not to configure SNMP, then the new radius/snmp/conf directory should remain empty.

Note that the syntax of the radius/snmp/conf/jnprsnmpd.conf file is particularly sensitive to the ordering of the parameters, malformed IP address CIDR notation, and stray white space. Misconfiguring this file will typically result in a broken SNMP agent. If you have stored any modified or third-party MIB files in the radius/snmp/mibs directory, these files should be migrated manually by copying them to the new Steel-Belted Radius software installation.

Manual Migration of Dictionaries

If you have stored any modified or third-party dictionary files (*.dci, *.dcm, *.dct) in the radius directory, then you must manually migrate these either by merging each of the modifications with the corresponding files that are shipped with the new Steel-Belted Radius software, or by copying the third-party dictionary files to the new radius directory.

Manual Migration of Third-Party Plug-ins and other Binaries

If you have stored any third-party plug-ins (*.so) and/or other binaries in the radius directory, then you must manually migrate them by copying the files to the new radius directory.

Uninstall the SBR Version 5.4 Administrator

When you upgrade from Steel-Belted Radius v5.4, the v5.4 Administrator is not uninstalled. It remains on the system, but it is no longer functional. It is recommended that you manually uninstall the old Administrator using the following procedure.

1. Issue the install_sbradmin_sol.sh command with the -uninstall argument.

```
root@quark:~/sbr> ./install_sbradmin_sol.sh -uninstall
SBR Administrator x.x Installer
```

(C) 2007 Juniper Networks, Inc.
All rights reserved.

Preparing to uninstall SBR Administrator x.x

The directory in which the software was installed
should contain .install_sbradmin.*timestamp*.dat

2. Identify the *radiusdir* directory.

   Enter directory to uninstall [/opt/funk]: **/opt/funk**

3. When you are asked to confirm you want to uninstall the SBR Administrator, enter **y**.

   Uninstall SBR Administrator 5.4 now [n]? **y**

   Uninstalling SBR Administrator 5.4
   Please wait...

   Unconfiguring

   SBR Administrator uninstalled, however files remain in /opt/funk

   Uninstall completed

4. After the installer indicates the SBR Administrator software has been uninstalled, archive or delete files remaining in the SBR Administrator directory.

Restoring a Previous Configuration

When you install the Steel-Belted Radius server software, the installation script saves your existing configuration to a backup directory to preserve your configuration settings. If you are re-installing the same version and edition of Steel-Belted Radius on a server, you can copy the configuration files from the backup directory to the Steel-Belted Radius server directory to restore your previous configuration.

If you are upgrading your Steel-Belted Radius software from an older version, do not copy your configuration files to the Steel-Belted Radius server directory. For more information, see “Upgrading from Steel-Belted Radius Versions 6.0 or 5.4” on page 34 or “The server does not restart itself automatically after a new license number is added. You must restart Steel-Belted Radius manually to activate the new license number. Refer to “Starting the RADIUS Server” on page 49 for information on how to restart your Steel-Belted Radius server.” on page 34, as appropriate.

Starting the RADIUS Server

Use the following command to start the RADIUS server manually.

cd *server-directory*
./sbrd start

If you change configuration settings for your Steel-Belted Radius server, you may need to restart Steel-Belted Radius to make the changes effective. As an alternative to issuing an sbrd stop command immediately followed by an sbrd start command, you can use the sbrd restart command to restart Steel-Belted Radius. When you issue the sbrd restart command, Steel-Belted Radius shuts down and then immediately starts the radius processes.

cd *server-directory*
./sbrd restart

Stopping the RADIUS Server

Use the following commands to stop the RADIUS server:

cd *server-directory*
./sbrd stop

When you execute the sbrd stop command, Steel-Belted Radius allows its subsystems to complete outstanding work and release resources, and then stops the radius processes gracefully.

If Steel-Belted Radius fails to stop after you issue the sbrd stop command, you can use the optional force argument to terminate all subsystems immediately.

cd *server-directory*
./sbrd stop force

Displaying RADIUS Status Information

You can use the sbrd status command to display status information for the RADIUS process.

cd *server-directory*
./sbrd status

Figure 3 illustrates the output of the sbrd status command.

Figure 3: Output of sbrd status Command

```
> sbrd status
ecarter 25927 .mkded start

—— Shared Memory Segments ——
key            shmid      owner      perms   bytes      nattch   status
0x42545256     891968     ecarter    600     8000000    2

—— Semaphore Arrays ——
key            semid      owner      perms   nsems
0x42545256     167116     ecarter    660     250

ecarter 2066 radius sbr.xml
radius processes are running
radius state is running
radius status 1101

Aggregate state is running
```

Chapter 5

Linux Installation

This chapter describes how to install or upgrade the Steel-Belted Radius server software on a Linux server. This chapter also describes how to install the optional SNMP software for use with the GEE and SPE editions of Steel-Belted Radius.

Before You Begin

- Verify that the proposed installation host complies with the hardware and software requirements of Steel-Belted Radius. For more information, see "System Requirements – Linux" on page 11.

- Make sure that you are (or have access to) a system administrator and someone who understands your RADIUS authentication and accounting requirements.

- If you are installing the optional SNMP module, stop all SNMP agents running on your server.

  NOTE: If your server runs SNMP agents other than the one supplied with Steel-Belted Radius, you must coordinate the port numbers used by your SNMP agents to avoid port contention.

- Past releases of Steel-Belted Radius on Linux platforms have used the btrieve database to store a significant portion of Steel-Belted Radius configuration data. The current release of SBR on Linux, v6.1, uses the raima database. Therefore, if you want to continue to use configuration data from past Steel-Belted Radius versions after you upgrade to v6.1, you must migrate your data as directed.

  The steps for migrating from the old database to the new database are included as part of the upgrade procedure. You must perform this migration in the order specified, after you install Steel-Belted Radius v6.1, but before you configure v6.1 and before you attempt to uninstall a previous Steel-Belted Radius version.

Upgrade Files

The install, configure, and uninstall scripts for Steel-Belted Radius version 6.1 automatically archive your Steel-Belted Radius files to the /radius/install/backups directory. To facilitate future software upgrades, the install, configure, and uninstall scripts create a number of .dat files in the /radius/install directory. These files store information used for future upgrades. You should not move, rename, or otherwise modify these files.

Table 8: Upgrade Files and Directories

File	Function
radius/install/package.dat	Contains a unique package identifier.
radius/install/preinstall.dat	Contains the absolute pathname of the backup directory for your old Steel-Belted Radius software and configuration files (pre-installation backup).
radius/install/install.dat	Contains the absolute pathname of the backup directory for your Steel-Belted Radius v6.1 software and configuration files, as shipped without modification (post-installation backup).
radius/install/upgrade.dat	Contains the absolute pathname of the Steel-Belted Radius version 6.1 upgrade source (if any).
radius/install/configure.dat	Contains configuration state data.
radius/install/uninstall.dat	Contains the absolute pathname of the backup directory for your Steel-Belted Radius v6.1 software and working configuration files (pre-uninstall backup).
radius/install/backups/	Contains the backups referenced by the.dat files.

Package Management Commands

Table 9 lists useful Linux package management commands.

Table 9: Useful Package Management Commands

Command	Function
rpm -q -a |egrep "FUNK|JNPR|RSAR"	Report any pre-existing packages and patches.
rpm -q -i sbr-gee-6.1.0-0	Report high level description for specified package
rpm -q –queryformat {INSTALLPREFIX}" sbr-gee-6.1.0-0	Show installed directory
rpm -i [–prefix */path*] sbr-gee.6.1.0-0.i386.lin.rpm	Install Steel-Belted Radius [at the specified */path*]. **NOTE:** The rpm -i command cannot be used to overwrite an existing installation.
rpm -U [–prefix */path*] sbr-gee.6.1.0-0.i386.lin.rpm	Upgrade an existing Steel-Belted Radius installation [in the specified */path*]
rpm -e sbr-gee-6.1.0-0	Uninstall Steel-Belted Radius.

Installing the Steel-Belted Radius Server Software

The installer for the Linux version of the Steel-Belted Radius server software uses RPM (Red Hat Package Manager) files, which have filenames that include the edition and version of the server software.

NOTE: This section assumes that you are installing Steel-Belted Radius on your Linux server for the first time or that you are installing Steel-Belted Radius in a directory other than the one used by previous installations (clean installation). If you are upgrading an existing Steel-Belted Radius installation to version 6.1, refer to "Upgrading from Steel-Belted Radius Versions 6.0 or 5.4" on page 59 for information on upgrade options and considerations.

To install the Steel-Belted Radius server software on a Linux server or workstation:

1. Log into the Linux server as root.

2. Copy the Steel-Belted Radius installation files to the Linux server.

   Make sure to copy them to a local or remote hard disk partition that is readable by root. The following example copies the files to the /opt/JNPRsbr/temp directory.

   ```
   # mkdir -p /opt/JNPRsbr/temp
   # cp -pR /cdrom/sbr/linux/* /opt/JNPRsbr/temp
   ```

3. Run the installer.

   # **rpm -i sbr-***XXX-version***.i386.lin.rpm**

   where *XXX* specifies the version of Steel-Belted Radius you want to install:

   - gee—Steel-Belted Radius/Global Enterprise Edition
   - spe—Steel-Belted Radius/Service Provider Edition
   - ent—Steel-Belted Radius/Enterprise Edition

   and *version* specifies the software version you want to install. For example, to run the RPM package used to install the GEE version of Steel-Belted Radius v6.1 to /opt/JNPRsbr, you would enter the following:

   # **rpm -i** ***/path/*sbr-gee-6.1.0-0.i386.lin.rpm**

   By default, the RPM package installs the Steel-Belted Radius files in the /opt/JNPRsbr directory. If you want to install Steel-Belted Radius in a directory other than /opt/JNPRsbr, you can use the –prefix option:

   # **rpm -i –prefix** *installdir* ***/path/*sbr-***edition-version*.**i386.lin.rpm**

4. Navigate to the directory where you installed Steel-Belted Radius.

   # cd /opt/JNPRsbr/radius/install

5. Execute the following command to run the configuration script for Steel-Belted Radius:

   # ./configure

6. Review the Steel-Belted Radius license agreement.

   Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter **y**.

   Do you accept the terms in the license agreement? [n] **y**

7. Indicate whether you have a license number.

   You can enter a license string or use a one-time 30 day trial license.
   Would you like to enter a license string? [n]

   - If you purchased Steel-Belted Radius, type **y** and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

   - If you do not have a license number, type **n** at the prompt and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product's full feature set for a limited period.

8. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI)

   Do you wish to enable LCI? [n]
   License does not have LCI support.

9. Specify whether you are upgrading an existing Steel-Belted Radius installation or configuring a new installation.

   - Enter n if you are performing a new installation.

   - Enter the directory path to the Steel-Belted Radius files if you are upgrading an existing Steel-Belted Radius installation and you know the name of the current Steel-Belted Radius directory.

   - Enter s if you are upgrading an existing Steel-Belted Radius installation and you want to search for the Steel-Belted Radius directory.

     Please enter backup or radius directory from which to upgrade.
     Enter n for new configuration, s to search, or q to quit.
     [n] **n**

10. Specify that you do not want to remove older versions of Steel-Belted Radius.

    ```
    WARNING: Now is the best time to remove any pre-existing versions of the
        software, as doing so later may destroy certain shared OS resources,
        such as /etc/init.d scripts in particular, that are about to be configured.
        Obsolete patches may also be removed.
    Manually remove pre-existing software now? [y]: n
    ```

11. Specify the login name of the initial Steel-Belted Radius administrator.

    The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

    ```
    Configuring for RedHat4
    Enter initial admin user (account must have an associated password) [root]:
    ```

NOTE: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

12. Specify whether you want to install the Steel-Belted Radius server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

    ```
    Configure SBR server as primary (p), replica (r), or stand alone (sa) [sa]: sa
    ```

    - If you enter p (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.

      If appropriate, enter **y** when you are asked whether you are upgrading a primary server. Doing so tells the installer to preserve the server's replication realm information.

    - If you enter r (replica server), you are prompted to specify how the replica server can locate the replica.ccmpkg configuration package containing your Steel-Belted Radius replication settings.

      - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.

      - If you want to specify the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address, and replication secret of the primary server.

    - If you enter sa (standalone RADIUS server), you do not need to specify replication information.

13. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

    - If you do not want to configure Steel-Belted Radius for use with an external LDAP data service, press Enter.

    - If you want to configure Steel-Belted Radius for use with an external LDAP data service, type **y** and press Enter. You are prompted to enter the path for the LDAP library files:

      ```
      Do you want to configure LDAP? [n]: y
      Enter path for LDAP library files [/usr/lib]:
      ```

    To accept the default path (/usr/lib), press Enter.

14. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can to monitor your Steel-Belted Radius server from an SNMP management station.

    ```
    Do you want to configure SNMP? [n]:
    ```

    If you do not want to install the optional SNMP module, press Enter to proceed to the next prompt.

    If you want to install the optional SNMP module, type **y** and press Enter. The configure script prompts you for the information it needs to configure the jnprsnmpd.conf and startsnmp.sh files.

    a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

       ```
       Choose a community string: public
       ```

    b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing (CIDR) format. To specify that only one host may query the agent, enter the IP address of the host followed by /32. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

       ```
       Specify the range of IPv4 addresses that may query this agent, such as
       1.2.3.0/24.
       Address range: 192.168.70.0/24
       ```

    c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the Steel-Belted Radius server.

       ```
       SNMPv2 trap sink: 192.168.70.86
       Configuration of SNMP complete.
       ```

NOTE: Refer to the *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

15. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

    ```
    Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1
    or later)? [n]:
    ```

NOTE: When you register your Steel-Belted Radius primary or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

16. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

    ```
    Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: e
    ```

    Steel-Belted Radius stores its autoboot settings in the local *radiusdir*\radius\sbrd file.

    - If you enter **e** (enable), the configure script copies the settings in the **sbrd** file to the **/etc/init.d** boot script and deletes old Steel-Belted Radius autoboot settings, thereby enabling autobooting for Steel-Belted Radius v6.1.
    - If you enter **d** (disable), the configure script does not copy the settings in the **sbrd** file to the **/etc/init.d** boot script and deletes old Steel-Belted Radius autoboot settings, thereby disabling autobooting for all versions of Steel-Belted Radius.
    - If you enter **p** (preserve), the configure script does not copy the settings in the **sbrd** file to the **/etc/init.d** boot script or delete old Steel-Belted Radius autoboot settings, thereby leaving your previous autoboot settings unchanged.

Next Steps

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

```
The SBR Administrator can be launched using the following URL:
http://<servername>:1812
Configuration complete
```

You must now finish configuring the new Steel-Belted Radius server to suit your network's authentication and accounting needs. For example, you can edit the [Addresses] section of the **radius.ini** file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the RADIUS process. Refer to "Starting the RADIUS Server" on page 78 for information on starting the RADIUS process. Refer to the *Steel-Belted Radius Administration Guide* for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

NOTE: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the Administrator has a secure configuration environment and direct access to certificates.

Upgrading from a 30-Day Trial Installation

You can download an evaluation version of Steel-Belted Radius from the Juniper website (http://www.juniper.net/products_and_services/). If you want to continue using the product at the end of the 30-day evaluation period, you do not need to re-install the software. You can add a license number to your existing installation to convert it from evaluation mode to licensed mode.

1. Purchase the Steel-Belted Radius software by contacting your preferred reseller or by contacting Juniper Networks. You will be shipped a product package that contains a license number.

2. Start the SBR Administrator and connect to your Steel-Belted Radius server.

   Refer to the *Steel-Belted Radius Administration Guide* for information on using the SBR Administrator.

3. Choose **File > License**.

4. When the Add a License for Server window opens, enter your license number and click **OK**.

   After you have entered a valid license number, the server displays a confirmation message and reminds you that you must restart the server.

5. Click **OK** to close the confirmation window.

6. Restart your Steel-Belted Radius server.

   The server does not restart itself automatically after a new license number is added. You must restart Steel-Belted Radius manually to activate the new license number. Refer to "Starting the RADIUS Server" on page 78 for information on how to restart your Steel-Belted Radius server.

Upgrading from Steel-Belted Radius Versions 6.0 or 5.4

NOTE: Steel-Belted Radius v6.1 only supports upgrades from v6.0 or v5.4. If you have a Steel-Belted Radius installation earlier than v5.4, you must first upgrade to v6.0 or v5.4 before you attempt to move to v6.1.

The procedure for upgrading your Steel-Belted Radius software has changed from previous (5.x) releases. Previously, you backed up and uninstalled your old Steel-Belted Radius software before installing new software. Steel-Belted Radius version 6.1 allows you to install your new software before deleting your old software. Steel-Belted Radius version 6.1 also helps you migrate your configuration and data files during the upgrade process.

Before You Begin

Before you upgrade your Steel-Belted Radius software from versions 5.4 or 6.0 to version 6.1 on a server, you should answer the following questions:

Where do you want to install your Steel-Belted Radius v6.1 software?

By default, Steel-Belted Radius v6.1 installs in the opt/JNPRsbr directory. You do not have to use the default installation directory. You can use the rpm --prefix *basedir* command to specify the target directory for Steel-Belted Radius installation.

When upgrading, note that the default installation directory for Steel-Belted Radius v5.4 software is /opt/funk directory. The default installation directory for Steel-Belted Radius v6.0 is /opt/JNPRsbr.

Do you want to retain your current Steel-Belted Radius configuration settings?

When you upgrade your Steel-Belted Radius software to version 6.1, you can start with the default Steel-Belted Radius configuration files, or you can choose to retain your current configuration files (data migration). The Steel-Belted Radius installer can create the following backups:

- Pre-installation backup—If you install Steel-Belted Radius v6.1 over a previous version, the installer copies your old software and configuration settings to a backup directory (*basedir*/radius/install/backups/*YYYY:MM:DD:HH:MM:SS*). The name of this pre-installation backup is recorded in the preinstall.dat file (described on page 52). The installer displays a message identifying the name of the pre-installation backup ("Existing server directory will be backed up as....")

- Post-installation backup—The installer always copies the default Steel-Belted Radius version 6.1 software and configuration settings to a backup directory (*basedir*/radius/install/backups/*YYYY:MM:DD:HH:MM:SS*). The name of this post-installation backup is recorded in the install.dat file (described on page 52). The installer displays a message identifying the name of the post-installation backup ("Newly installed server directory will be backed up as....")

If you want to preserve your previous version configuration settings, you can tell the configure script to migrate your settings from the pre-installation directory (or from another backup directory) to the working (/radius) directory. You would then copy parameters from the default version 6.1 configuration files in the post-installation backup to your configuration files to set up new Steel-Belted Radius features.

NOTE: Steel-Belted Radius v6.1 uses the raima database rather then the btreive database used in previous versions. Therefore, in order to use your previous version configuration data for use with v6.1, you must migrate your data by running a utility called dbconvert during the upgrade process. dbconvert is a conversion tool that creates a new Steel-Belted Radius v6.1-compatible RDM database from content in the pervasive btrieve database files used in previous versions of Steel-Belted Radius. Refer to "Use dbconvert to Migrate the btrieve Database to the raima Database" on page 67 when upgrading.

If you want to start with the default Steel-Belted Radius v6.1 settings, you can tell the configure script to skip the data migration and install the default version 6.1 configuration files. You could then merge settings from the archive files in the pre-installation backup directory to the default files to re-create your current configuration.

NOTE: Do not modify the backup directories or the .dat files that identify them. If you do, you may have difficulty upgrading your Steel-Belted Radius software in the future.

If upgrading, is your current version of Steel-Belted Radius running on a platform that is supported by the v6.1 release?

If not, you must first migrate SBR to a supported platform as is detailed in "Moving Steel-Belted Radius to another Operating System" on page 75 before upgrading.

Do you want to retain your old Steel-Belted Radius software on your server?

During the configuration process, you will be asked whether you want to uninstall your old Steel-Belted Radius software. If you indicate that you do, the configure script will terminate so you can uninstall your old software manually. After you have uninstalled your old Steel-Belted Radius software, you can restart the configuration script to resume the installation/configuration process.

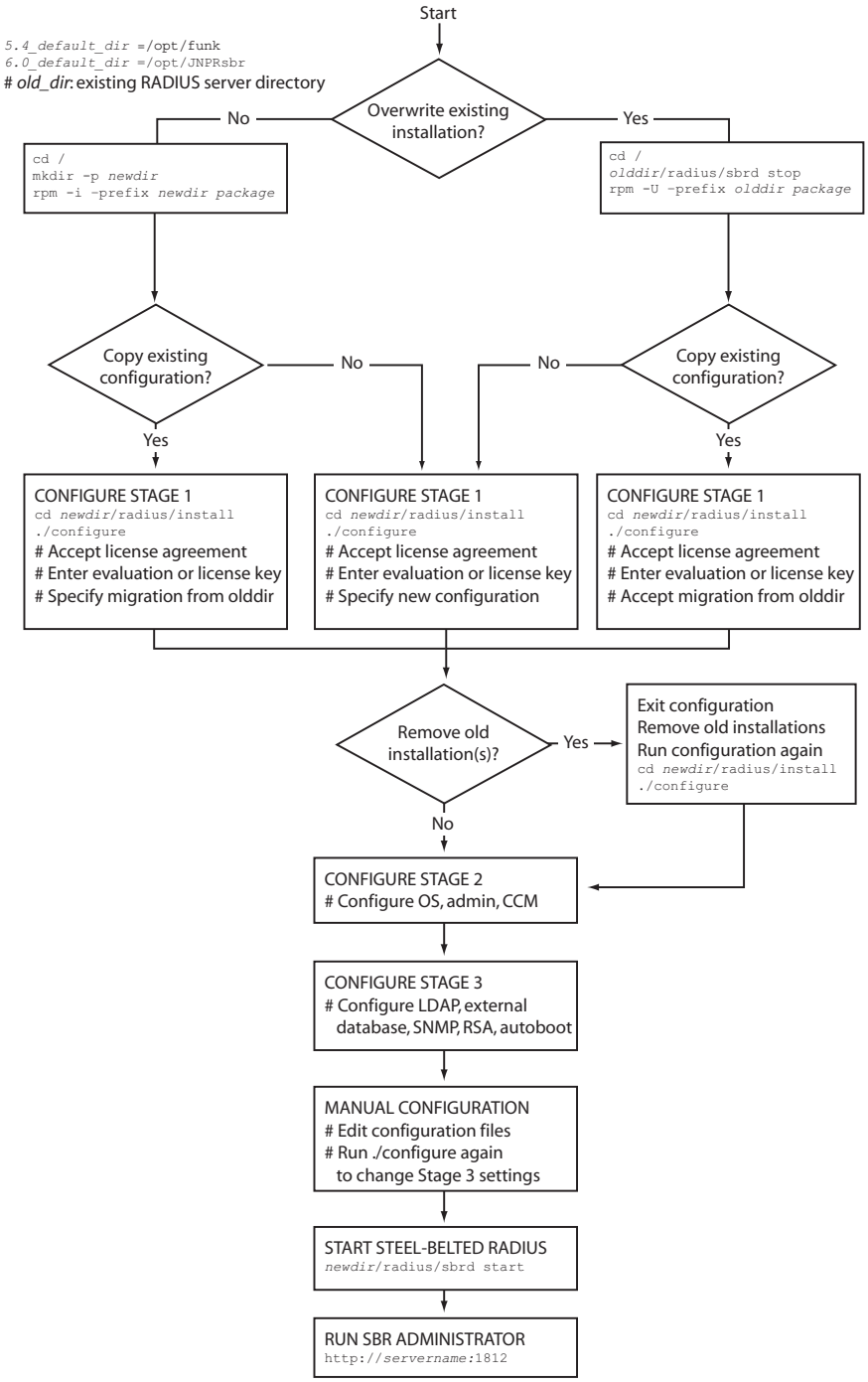
Figure 4 presents a decision tree that summarizes the choices you make and tasks you perform when upgrading from Steel-Belted Radius v6.0 or v5.4 to Steel-Belted Radius v6.1.

The configuration process consists of three phases. Note the following:

- In Stage 1, you specify whether you want to use your current data files to configure Steel-Belted Radius (data migration). After Stage 1 is complete, you will be asked whether you want to delete your old Steel-Belted Radius software.
- In Stage 2, you specify a default administrator and a centralized configuration management (CCM) role (stand-alone, primary server, or replica server).

- In Stage 3, you specify configuration information for LDAP, external databases, SNMP, autoboot (**sbrd** script), and whether you want your server to function as an Agent Host with RSA Authentication Manager. If you re-run the configure script in the future, it will automatically start at Stage 3.

Figure 4: Decision Tree for Steel-Belted Radius Upgrades (Linux version)



The following scenarios apply to upgrading from v5.4 to v6.1 as follows:

- Scenario 1 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/funk directory) that retains the existing configuration information. The old software is archived and overwritten with the new software. The default version 6.1 configuration files are copied to the /opt/funk/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 2 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the software in the old /opt/funk directory is preserved) that retains the existing configuration information. The default version 6.1 configuration files are copied to the /opt/JNPRsbr/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 3 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that retains the existing configuration information. The default version 6.1 configuration files are copied to the /opt/JNPRsbr/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 4 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/funk directory) that installs clean (default) version 6.1 configuration files. The old software and configuration settings are archived in the /opt/funk/radius/install/backups/*YYYY:MM:DD-HH:MM:*SS directory; you can use your archived configuration files to merge customized settings into your new configuration files manually.

- Scenario 5 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the software in the old /opt/funk directory is preserved) that installs clean (default) version 6.1 configuration files. You can merge customized settings from your old configuration files into your new configuration files manually. This scenario would be appropriate in situations where you want to install and experiment with a new release of Steel-Belted Radius before discarding older releases.

- Scenario 6 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in the new /opt/JNPRsbr directory and the old /opt/funk directory is deleted) that installs clean (default) version 6.1 configuration files. If you archived your old settings manually, you can use your archived configuration files to merge customized settings into your new configuration files.

The following scenarios apply to upgrading from v6.0 to v6.1 as follows:

- Scenario 1 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/JNPRsbr directory) that retains the existing configuration information. The old software is archived and overwritten with the new software. The default version 6.1 configuration files are copied to the /opt/JNPRsbr /radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 2 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is not installed in the default directory, but in a directory of your choosing, and the old /opt/JNPRsbr directory and the software in the old /opt/JNPRsbr directory are both preserved) that retains the existing configuration information. The default version 6.1 configuration files are copied to the newdir/radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use these files to merge new settings into your configuration files manually.

- Scenario 3 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in a directory of your choosing and the old /opt/JNPRsbr directory is deleted) that retains the existing configuration information. The default version 6.1 configuration files are copied to the newdir/radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use these files to merge new settings into your configuration files manually.

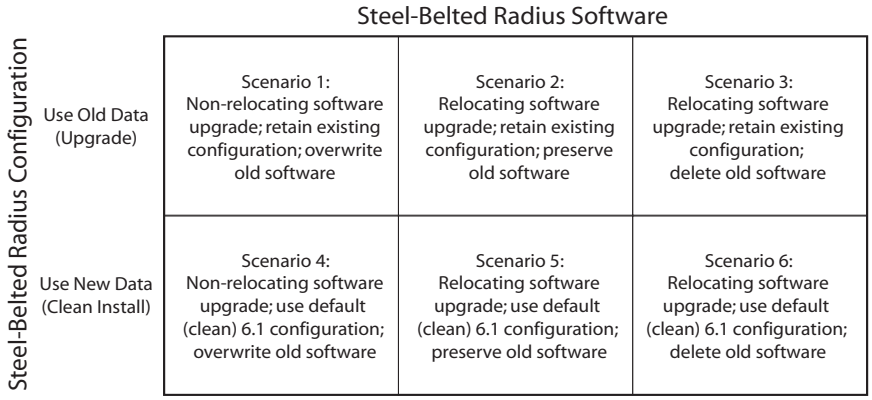
- Scenario 4 illustrates a non-relocating software upgrade (meaning that the version 6.1 software is installed in the old /opt/JNPRsbr directory) that installs clean (default) version 6.1 configuration files. The old software and configuration settings are archived in the /opt/JNPRsbr/radius/install/backups/*YYYY:MM:DD-HH:MM:SS* directory; you can use your archived configuration files to merge customized settings into your new configuration files manually.

- Scenario 5 illustrates a non-destructive relocating software upgrade (meaning that the version 6.1 software is installed in a directory of your choosing and the /opt/JNPRsbr directory and the software in the old /opt/JNPRsbr directory are both preserved) that installs clean (default) version 6.1 configuration files. You can merge customized settings from your old configuration files into your new configuration files manually. This scenario would be appropriate in situations where you want to install and experiment with a new release of Steel-Belted Radius before discarding older releases.

- Scenario 6 illustrates a destructive relocating software upgrade (meaning that the version 6.1 software is installed in a directory of your choosing and the old /opt/JNPRsbr directory is deleted) that installs clean (default) version 6.1 configuration files. If you archived your old settings manually, you can use your archived configuration files to merge customized settings into your new configuration files.

Figure 5 presents this decision process as a set of upgrade scenarios:

Figure 5: Upgrade Scenarios


Steel-Belted Radius Software
Steel-Belted Radius Configuration
Use Old Data (Upgrade)
Use New Data (Clean Install)
Scenario 1: Non-relocating software upgrade; retain existing configuration; overwrite old software
Scenario 2: Relocating software upgrade; retain existing configuration; preserve old software
Scenario 3: Relocating software upgrade; retain existing configuration; delete old software
Scenario 4: Non-relocating software upgrade; use default (clean) 6.1 configuration; overwrite old software
Scenario 5: Relocating software upgrade; use default (clean) 6.1 configuration; preserve old software
Scenario 6: Relocating software upgrade; use default (clean) 6.1 configuration; delete old software

Begin the Upgrade Procedure

Perform the following steps to upgrade your Steel-Belted Radius software from version 6.0 or 5.4 to version 6.1 on a server running RedHat Linux. Note that as part of the upgrade process, you must also run a utility called dbconvert to move old configuration data you preserving from the btrieve database to the new raima database used in v6.1. Those instructions are included with the upgrade procedure.

NOTE: Do not uninstall your existing version of Steel-Belted Radius before upgrading to v6.1.

NOTE: If the version of Steel-Belted Radius you are upgrading is running on a platform that is not supported by the Steel-Belted Radius v6.1 release (namely Red Hat 3), you don't perform an upgrade. Instead, if you want to preserve your configuration, you should export your data and then import it to v6.1 as detailed in "Moving Steel-Belted Radius to another Operating System" on page 75.

1. Log into the Linux server as root.

2. Stop the RADIUS process currently running on your server.

   For v6.0:
   #/opt/JNPRsbr/radius/sbrd stop

   or

   For v5.4:
   # /opt/funk/radius/sbrd stop

3. Back up your */radiusdir* directory to an archive location.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup. This backup directory is needed for data migration tasks that are associated with future upgrades.

```
# cd /opt/JNPRsbr
# mkdir /opt/backups
# tar cf - radius | ( cd /opt/backups; tar xfBp - )
```

or

```
# cd /opt/funk
# mkdir /opt/backups
# tar cf - radius | ( cd /opt/backups; tar xfBp - )
```

4. Back up your root and server certificates, and verify you know the password for your server certificate.

   You will install your server certificate for Steel-Belted Radius v6.1 by running the SBR Administrator configuration application.

5. Copy the Steel-Belted Radius installation files to the Linux server. Make sure to copy them to a local or remote hard disk partition that is readable by root. The following example copies the files to the /opt/JNPRsbr/temp directory; you can use any directory you choose.

   ```
   # mkdir -p /opt/JNPRsbr/temp
   # cp -pR /cdrom/sbr/linux/* /opt/JNPRsbr/temp
   ```

6. If you installed the 969531-01 or 969541-01 security patch for Steel-Belted Radius v5.4, uninstall the security patch.

   You must uninstall the security patch manually, using the appropriate package removal command (rpm -e).

7. Run the installer for the Steel-Belted Radius v6.1 server software.

   7A. Non-relocating installation: If you want to install your Steel-Belted Radius v6.1 software in the directory that contains your Steel-Belted Radius version 6.0 or 5.4 software (overwriting your current Steel-Belted Radius software with the version 6.1 software), execute the following command:

   rpm -U --prefix /opt/JNPRsbr sbr-*XXX-version*.i386.lin.rpm

   or

   rpm -U --prefix /opt/funk sbr-*XXX-version*.i386.lin.rpm

   where *XXX* specifies the edition of Steel-Belted Radius you want to install:

   - gee—Steel-Belted Radius/Global Enterprise Edition
   - spe—Steel-Belted Radius/Service Provider Edition
   - ent—Steel-Belted Radius/Enterprise Edition

   and *version* specifies the software version you want to install. For example:

   rpm -U --prefix /opt/JNPRsbr sbr-gee-6.1.0.i386.lin.rpm

7B. Relocating installation: If you want to install your Steel-Belted Radius v6.1 software in a directory other than the one containing your Steel-Belted Radius version 6.0 or 5.4 software, execute the following command:

rpm -i [--prefix *installdir*] sbr-*XXX-version*.i386.lin.rpm

8. Navigate to the directory where you installed Steel-Belted Radius and run the configuration script for Steel-Belted Radius.

   # cd /opt/JNPRsbr/radius/install
   # ./configure

9. Review the Steel-Belted Radius license agreement.

   Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter **y**.

   Do you accept the terms in the license agreement? [n] **y**

10. Indicate whether you have a license number.

    You can enter a license string or use a one-time 30 day trial license.
    Would you like to enter a license string? [n]

    - If you purchased Steel-Belted Radius, type **y** and press Enter. When prompted to do so, enter your license number and press Enter. (Your license number can be found on a sticker affixed to the license agreement in your product package.) The script creates your license file and copies it to your server directory.

    - If you do not have a license number, type **n** at the prompt and press Enter. The Steel-Belted Radius software is installed as a 30-day evaluation package, allowing use of the product's full feature set for a limited period.

11. If you are installing the Enterprise Edition (EE) of Steel-Belted Radius with a trial license, specify whether you want to enable the LDAP configuration interface (LCI).

    Do you wish to enable LCI? [n]
    License does not have LCI support.
    Installed a 30 day evaluation license.

12. You are next prompted to do the following:

    Please enter backup or radius directory from which to migrate.
    Enter n for new configuration, s to search, or q to quit
    [/opt/JNPRsbr/radius/install/backups/2007:09:24-13:34:21]:

    WARNING: the specified migration source contains btrieve data
    HINT: Execute dbconvert before attempting to configure again.

    Manually execute dbconvert now? [y]:

    Please execute configure again when you are finished

You should now run the dbconvert utility as described in the following section.

Use dbconvert to Migrate the btrieve Database to the raima Database

If you are migrating your old configuration data, you must run dbconvert at this point in the upgrade process, before you configure Steel-Belted Radius v6.1.

dbconvert is a conversion tool that creates a new Steel-Belted Radius v6.1-compatible RDM database from content in the Pervasive btrieve database files used in previous versions of Steel-Belted Radius. dbconvert consists of a single executable file and can be run from any directory. You can use the -p command line option to specify a pathname where the btrieve database and the btrieve shared library files are found (in other words, the SBR service directory.) If no pathname is specified, dbconvert will look in the current directory for these files.

Once Steel-Belted Radius v6.1 is installed, you can invoke the dbconvert utility with option -h in order to review its usage information as follows:

```
/opt/JNPRsbr/radius/dbconvert -h

USAGE:      non-relocating upgrade: ./dbconvert
            relocating upgrade: ./dbconvert [old radius directory]
```

If you are performing a relocating upgrade, specify the absolute path of the old radius directory, for example: /opt/JNPRsbr/radius (Note that this is slightly different from the Linux rpm utility's -prefix option which specifies the absolute path to the directory that contains the radius directory, for example. /opt/JNPRsbr).

If you are performing a non-relocating upgrade, you do not need to specify any arguments (no arguments are synonymous with any path to the new radius directory or any path to the pre-install backup of the old Steel-Belted Radius release). Note that you must first change your working directory to the new radius directory before you invoke the dbconvert utility.

To perform a relocating upgrade, execute the following commands:

```
su -
cd /opt/JNPRsbr/radius
./dbconvert /opt/funk/radius
```

To perform a non-relocating upgrade, execute the following commands:

```
su -
cd /opt/JNPRsbr/radius
./dbconvert
```

The dbconvert utility restores the btrieve database from backup to the current working directory and, if needed, initializes the Raima database (also in the current working directory), and invokes the conversion process. If the database conversion is attempted more than once, or if you manually restore the btrieve database to the current working directory, then the dbconvert utility will abort, complaining that btrieve and/or raima files already exist. In this case, you may use the dbconvert -i option to enable interactive mode, so that you can instruct dbconvert whether to remove (and subsequently overwrite) the existing files or to reuse the existing files.

Refer to the following conversion output example:

```
restoring btrieve
/opt/JNPRsbr/radius/btrieve
remove existing file or directory (above)? [n]: y
/opt/JNPRsbr/radius/radads.dat
remove existing file or directory (above)? [n]: y
/opt/JNPRsbr/radius/radclnt.dat
remove existing file or directory (above)? [n]: y
/opt/JNPRsbr/radius/radiusdata.d01
/opt/JNPRsbr/radius/radiusdata.d02
/opt/JNPRsbr/radius/radiusdata.d03
/opt/JNPRsbr/radius/radiusdata.dbd
/opt/JNPRsbr/radius/radiusdata.k01
/opt/JNPRsbr/radius/radiusdata.k02
/opt/JNPRsbr/radius/vista.taf
dbconvert: WARNING: conversion would overwrite existing raima data files
(above)
ignore and proceed anyway? [n]: y
btrieve state is stopped
waiting for btrieve
btrieve started
initializing raima data
starting conversion process
2007/8/9 12:26:06 Starting database conversion tool, version 0.1
2007/8/9 12:26:06 Btrieve Client requestor, version 8.60
2007/8/9 12:26:06 Btrieve 32-bit Windows workstation/workgroup engine or
Linux server using Workgroup authentication mode, version 8.60
2007/8/9 12:26:06 SBR database conversion was successful.
finished conversion process
btrieve state is running
waiting for btrieve
btrieve stopped
removing btrieve shared IPC objects
removing btrieve temporary files
removing btrieve lock files
```

The message "starting conversion process" in the example indicates that a database conversion was attempted. When the conversion is complete, you should examine the dbconvert.log file (found in the current working directory) for possible conversion errors. If the conversion was successful, the dbconvert.log file is empty. If any conversion errors are listed in the log file, then the database conversion is probably incomplete or in question. You should correct all conversion errors before continuing. If you wish to continue despite any conversion errors, then you can use the dbconvert -c option to ignore errors.

You should also make a note of the path that is recorded in the install/dbconvert.dat file. This path is the location from which the old btrieve database was obtained. To ensure consistency between the Steel-Belted Radius configuration data that is stored in the database and other Steel-Belted Radius configuration files, you should specify this same path when the new Steel-Belted Radius software is configured at a later time. This path should be the default when the configure script eventually prompts you as follows:

```
Please enter backup or radius directory from which to migrate.
Enter n for new configuration, s to search, or q to quit
```

[/opt/JNPRsbr/radius]:

Once you are satisfied that the database conversion was successful, proceed with the upgrade.

Finalize the Upgrade Procedure

13. You must now run /.configure again and accept the End User License Agreement again.

    # cd install
    # ./configure

14. Review the Steel-Belted Radius license agreement.

    Press the spacebar to move from one page to the next. When you are prompted to accept the terms of the license agreement, enter **y**.

    Do you accept the terms in the license agreement? [n] **y**

15. Specify whether you want to migrate your current Steel-Belted Radius configuration files.

    - If you are performing a non-relocating update (or if you are performing a relocating update and you want to migrate your configuration files), specify the directory path to your current Steel-Belted Radius files. If you are performing a non-relocating update, the default is the pre-installation backup of your current settings.

      Please enter backup or radius directory from which to upgrade.
      Enter n for new configuration, s to search, or q to quit.
      [/*radiusdir*/radius/install/backups/*timestamp*]

      Press Enter to accept the default value, or enter a different path if you want to use a different set of configuration files. You can enter **s** if you want to search for the directory path for your Steel-Belted Radius files.

    - If you do not want to migrate your configuration files, enter **n** to specify that you want to use the default configuration files.

      Please enter backup or radius directory from which to upgrade.
      Enter n for new configuration, s to search, or q to quit.
      [n] **n**

16. Specify whether you want to remove your old Steel-Belted Radius software.

    If you want to remove your old Steel-Belted Radius software, enter **y** at the Manually remove pre-existing software now? prompt, uninstall the old software, and then run the configuration script again. When you restart the configuration script, the script returns you to this step.

    ```
    WARNING: Now is the best time to remove any pre-existing versions of the
        software, as doing so later may destroy certain shared OS resources,
        such as /etc/init.d scripts in particular, that are about to be configured.
        Obsolete patches may also be removed.
    Manually remove pre-existing software now? [y]: y
    ```

17. Specify the login name of the initial Steel-Belted Radius administrator.

    The account information you enter is the default login account for the SBR Administrator. You must use this account name the first time you log into the SBR Administrator.

    ```
    Enter initial admin user (account must have an associated password) [root]:
    ```

NOTE: Make sure the login account you specify has a password. If you specify a user without a password as the administrator, you will not be able to log into the SBR Administrator.

18. If you are not migrating your old configuration data, specify whether you want to install the Steel-Belted Radius server as a primary server (p), a replica server (r), or a standalone RADIUS server (sa).

    ```
    Configure SBR server as primary (p), replica (r), or stand alone (sa) [sa]: r
    ```

    - If you enter p (primary server), you are prompted to enter the replication secret used to authenticate communications between the primary server and replica servers. Enter and confirm the replication secret and press Enter to continue.
    - If you enter r (replica server), you are prompted to specify how the replica server can locate the replica package containing your Steel-Belted Radius replication settings.
        - If the replication package is present on your computer or network, you are prompted to specify the path to the replica.ccmpkg file.
        - If you want to specify the location of the primary server (from which the replica server can copy its replication package automatically), enter the name, IP address(es), and replication secret of the primary server.
    - If you enter sa (standalone RADIUS server), you do not need to specify replication information.

19. Specify whether you want to configure Steel-Belted Radius for use with an external LDAP data service.

    ```
    Do you want to configure LDAP? [n]:
    ```

- If no, press Enter.
- If yes, type **y** and press Enter. You are prompted to enter the path for the LDAP library files:

Enter path for LDAP library files [/usr/lib]:

To accept the default path (/usr/lib), press Enter.

20. If you are installing the Service Provider Edition (SPE) or Global Enterprise Edition (GEE) of Steel-Belted Radius, specify whether you want to install the optional SNMP module so that you can to monitor your Steel-Belted Radius server from an SNMP management station.

    Do you want to configure SNMP? [n]:

    If no, press Enter to proceed to the next prompt.

    If yes, type **y** and press Enter. The configure script prompts you for the information it needs to configure the jnprsnmpd.conf and startsnmp.sh files.

    a. When you are prompted for a community string, enter the community string used to validate information sent from the SNMP subagent on the Steel-Belted Radius server to your SNMP management station.

       Choose a community string: **public**

    b. When you are prompted for a range of IPv4 addresses, specify a starting IP address in Classless Inter-Domain Routing (CIDR) format. To specify that only one host may query the agent, enter the IP address of the host followed by /32. To specify that any host on a designated class C network may query the agent, enter the starting address of the network followed by /24.

       Specify the range of IPv4 addresses that may query this agent, such as 1.2.3.0/24.
       Address range: **192.168.70.0/24**

    c. If you are using SNMPv2, enter the DNS name or IP address of the trap sink that will receive trap information from the Steel-Belted Radius server.

       SNMPv2 trap sink: **192.168.70.86**
       Configuration of SNMP complete.

NOTE: Refer to the *Steel-Belted Radius Administration Guide* for information on configuring the SNMP agent.

21. Specify whether you want to register your Steel-Belted Radius server as an Agent Host with RSA Authentication Manager.

    Do you want register SBR with an RSA server (requires RSA Auth Manager 6.1 or later)? [n]:

NOTE: When you register your Steel-Belted Radius primary or replica server as an Agent Host with an RSA SecurID server, it registers itself as an RSA replica. This is normal behavior.

22. Specify whether you want to configure the Steel-Belted Radius server to autoboot (restart automatically when the operating system is restarted).

    Enable (e), disable (d), or preserve (p) RADIUS autoboot [e]: **e**

    - If you enter **e**, the configure script saves the **sbrd** script and copies it to the **/etc/init.d** boot script.
    - If you enter **d**, the configure script discards changes made to the **sbrd** script.
    - If you enter **p**, the configure script saves the **sbrd** script and but does not copy it to the **/etc/init.d** boot script.

When you finish entering settings, the script configures Steel-Belted Radius with the settings you specified.

```
The SBR Administrator can be launched using the following URL:
http://<servername>:1812
Configuration complete
```

You must now finish configuring the new Steel-Belted Radius server to suit your network's authentication and accounting needs. For example, you can edit the [Addresses] section of the **radius.ini** file to specify the IP addresses that you want Steel-Belted Radius to use. Refer to the *Steel-Belted Radius Reference Guide* for information on how to edit the configuration files used by Steel-Belted Radius.

After you have updated your Steel-Belted Radius configuration files, you can run SBR Administrator to enter information about your users and RADIUS clients, set up EAP authentication methods, add a server certificate, and configure other settings. Before you can run SBR Administrator, you must start the **radius** process. Refer to "Starting the RADIUS Server" on page 78 for information on starting the RADIUS process. Refer to the *Steel-Belted Radius Administration Guide* for information on how to use SBR Administrator to configure your Steel-Belted Radius server.

NOTE: It is recommended that you run the SBR Administrator locally when configuring the server. This way, the Administrator has a secure configuration environment and direct access to certificates.

Additional Required Manual File Upgrades

Upgrading from v6.0 or v5.4 to v.61 requires some additional, manual upgrading of certain configuration files. The files and file types listed in this section are those that require manual migration. All other files are automatically migrated during the upgrade process or the configuration export/import process.

Manual Migration of XML configurations

You must manually migrate the following XML files by merging any changed values into the corresponding XML files that are shipped with the new Steel-Belted Radius software installation (you should never modify any other *.xml files):

- radius/sbr_administration.xml - socket port number specified by port = setting
- radius/sbr_ccm.xml - socket port numbers specified by port = settings
- radius/sbr_id.xml - hostname specified by id = setting
- system/config/logging_mgr.xml - logStream events = settings

The IP addresses, hostnames, socket port numbers, and other similar data entries found in these files often have corresponding parameters in the radius.ini file which must be kept in agreement.

Manual Migration of JRE Extensions

Steel-Belted Radius ships its own Java Runtime Environment (JRE) for the purposes of facilitating JDBC plug-ins and Java Scripting. You can extend the JRE by installing third-party .jar files in the radius/jre/lib/ext subdirectory. You must migrate any third-party .jar files by copying them to the new Steel-Belted Radius software installation.

Note that the following .jar files are shipped with Steel-Belted Radius and should not be migrated:

- dnsns.jar
- funk-sql.jar
- localedata.jar
- sunjce_provider.jar
- sunpkcs11.jar
- ldapsec.jar (5.4 release only)

Manual Migration of JavaScript files

As of v5.4, all JavaScript files (*.jsi) are stored in the radius/scripts subdirectory. Any JavaScript files must be migrated manually to v6.1 by copying them to the new Steel-Belted Radius software installation.

Manual Migration of ROOT Certificates

As of v5.4, the storage of root certificates is managed by the Steel-Belted Radius server and the SBR Administrator is used to add and delete root certificates. You must manually migrate root certificates by using the SBR Administrator to add them from the old root directory.

Manual Migration of SNMP Configuration

SNMP configuration is contained in the radius/snmp/conf directory (for example radius/snmp/conf/jnprsnmpd.conf). You must manually migrate this configuration by merging the contents of the files into the files that are shipped with the new Steel-Belted Radius software installation. But if you choose not to configure SNMP, then the new radius/snmp/conf directory should remain empty.

Note that the syntax of the radius/snmp/conf/jnprsnmpd.conf file is particularly sensitive to the ordering of the parameters, malformed IP address CIDR notation, and stray white space. Misconfiguring this file will typically result in a broken SNMP agent. If you have stored any modified or third-party MIB files in the radius/snmp/mibs directory, these files should be migrated manually by copying them to the new Steel-Belted Radius software installation.

Manual Migration of Dictionaries

If you have stored any modified or third-party dictionary files (*.dci, *.dcm, *.dct) in the radius directory, then you must manually migrate these either by merging each of the modifications with the corresponding files that are shipped with the new Steel-Belted Radius software, or by copying the third-party dictionary files to the new radius directory.

Manual Migration of Third-Party Plug-ins and other Binaries

If you have stored any third-party plug-ins (*.so) and/or other binaries in the radius directory, then you must manually migrate them by copying the files to the new radius directory.

NOTE: You may choose whether or not to migrate accounting files (radius/*.act) and log files (radius/*.log, radius/audit/*, radius/authReports/*).

Uninstall the SBR Version 5.4 Administrator

When you upgrade from Steel-Belted Radius v5.4, the v5.4 Administrator is not uninstalled. It remains on the system, but it is no longer functional. It is recommended that you manually uninstall the old Administrator using the following procedure.

1. Issue the install_sbradmin_lin.sh command with the -uninstall argument.

```
root@quark:~/sbr> ./install_sbradmin_lin.sh -uninstall
SBR Administrator x.x Installer
(C) 2007 Juniper Networks, Inc.
All rights reserved.
Preparing to uninstall SBR Administrator x.x
The directory in which the software was installed
should contain .install_sbradmin.timestamp.dat
```

2. Identify the *radiusdir* directory.

   Enter directory to uninstall [/opt/funk]: **/opt/funk**

3. When you are asked to confirm you want to uninstall the SBR Administrator, enter **y**.

   Uninstall SBR Administrator 5.4 now [n]? **y**

   Uninstalling SBR Administrator 5.4
   Please wait...

   Unconfiguring

   SBR Administrator uninstalled, however files remain in /opt/funk

   Uninstall completed

4. After the installer indicates the SBR Administrator software has been uninstalled, archive or delete files remaining in the SBR Administrator directory.

Moving Steel-Belted Radius to another Operating System

The Linux release of Steel-Belted Radius v6.1is supported on RedHat 4. Older Steel-Belted Radius versions were supported on RedHat 3. If you are upgrading a version of Steel-Belted Radius that is running on Red Hat 3 and you want to preserve and use your existing configuration data, you must move it to the new operating system.

The following procedure assumes you are moving Steel-Belted Radius configuration data from one machine (source) to another machine (target) as part of an OS version change and upgrade to v6.1. Information for upgrading an OS in place, on the same system, is detailed in "Upgrading in Place to Another Operating System" on page 78.

NOTE: If you are planning to upgrade an Steel-Belted Radius cluster, the existing primary node should always be upgraded first. Once the newly migrated primary node is functioning, delete all existing replica nodes from the newly upgraded primary node's CCM server list. The existing replica nodes should be upgraded last, and the newly upgraded primary node specified when the newly upgraded replicas are installed and configured. Once functioning, the newly upgraded replica nodes will contact the newly upgraded primary node, thus re-populating the primary node's CCM server list and re-synchronizing the newly upgraded Steel-Belted Radius cluster. Once the newly upgraded Steel-Belted Radius cluster is functioning, you can decommission the existing Steel-Belted Radius cluster.

Moving Configuration Data to Another Operating System

NOTE: If this is a primary node, be sure to delete all existing replica nodes from the newly migrated primary node's CCM server list. If this is a replica node, verify that it has contacted the newly migrated primary node as opposed to the existing primary node.

When moving configuration data to a new OS for the purpose of upgrading to Steel-Belted Radius v6.1, you should do the following tasks in the order listed:

On the RedHat 3 system, export SBR configuration data from the older Steel-Belted Radius version to an XML file as follows:

1. Run the SBR Administrator.
2. Choose **File > Export**.
3. When the Export dialog opens, select the information you want to export.

   Each tab in the dialog lists exportable items of a particular category. For each category, select the appropriate tab and click each item you'd like to export.

   To select a contiguous range of items, select the first item in the range, hold down the Shift key, and click the last item in the range.

   To select a non-contiguous set of items, hold down the Ctrl key as you click each item you want.

   To select all items in a category, click **All**.

   To select all items in all categories, click **Select All**.
4. After you have selected the items you want to export, click **OK**.
5. When the Export to XML dialog opens, specify a file name and click **Save**.
6. On the RedHat 3 system, stop the Steel-Belted Radius service as follows:

   cd *server-directory*

   ./sbrd stop
7. On the RedHat 4 system, install Steel-Belted Radius v6.1 by following the instructions in “Installing the Steel-Belted Radius Server Software” on page 53.
8. On the RedHat 4 system with new Steel-Belted Radius v6.1 installation, execute **radius/install/configure**.
9. On the RedHat 4 system, stop the Steel-Belted Radius service as follows:

   cd *server-directory*

   ./sbrd stop

10. Manually copy the Steel-Belted Radius configuration files that are not part of the import XML file from the RedHat3 system to the RedHat 4 system. Those files, located in the radius directory, have the following extensions:

    .ini, .dcm, .dct, .dci, .pfx, .der, .aut, .eap, .dir, .pro, .dhc, .rr, .rl, .ctrl, .acc, .att, .conf, .gen, .jsi, and .ses

    You should also copy the acthdr.dat and sdconf.rec files.

    See "Additional Required Manual File Upgrades" on page 73 for the full list of files you should copy. Pay special attention to those files that you should not overwrite.

11. On the RedHat 4 system, start the Steel-Belted Radius service as follows:

    cd *server-directory*

    ./sbrd start

On the RedHat 4 system, import Steel-Belted Radius configuration data from the older Steel-Belted Radius version to the new Steel-Belted Radius v6.1 installation as follows:

12. Run the SBR Administrator.

13. Choose **File > Import**.

14. When the Import from XML dialog opens, select the XML file containing the information you want to import and click **Open**.

15. When the Import dialog opens, specify whether what the SBR Administrator should do when it finds an object with the same name in the Steel-Belted Radius database.

    - Click **Skip** if you want SBR Administrator to leave the item already in the database intact.
    - Click **Replace** if you want SBR Administrator to overwrite the item in the database with the imported information.

16. Select the information you want to import by clicking each tab and selecting items to import.

    To select a contiguous range of items, select the first item in the range, hold down the Shift key, and click the last item in the range.

    To select a non-contiguous set of items, hold down the Ctrl key as you click each item you want.

    To select all items in a category, click **All**.

    To select all items in all categories, click **Select All**.

17. After you select all the items you want, click **OK**. The items you selected are added to the Steel-Belted Radius database.

Now your Steel-Belted Radius v6.1 installation is complete with all configuration data from the previous version available to you.

Upgrading in Place to Another Operating System

If you intend to upgrade the OS on the current machine in which Steel-Belted Radius is installed and running, it is recommended that you follow the procedure described in "Moving Steel-Belted Radius to another Operating System" on page 75 for migrating Steel-Belted Radius. Attempting to upgrade the OS with Steel-Belted Radius in place and expecting Steel-Belted Radius to function normally after the OS upgrade is an unlikely scenario and not the recommended procedure.

When doing this, you should be aware of the following:

- In order to prevent a catastrophic loss of data, most OS manufacturers recommend that you back up the entire OS and all file systems before attempting to upgrade the OS. The Steel-Belted Radius software must be stopped while backups are created and while the OS is upgraded.
- If the server-type is replica, make sure that the primary node has already been migrated as needed. The primary node must be specified when a replica node is configured, and the replica node will contact the primary node when it is started.
- You should perform upgrade tasks in the following order:
  - Export existing configuration to an XML file and move that file off the system. Refer to the instructions in "Moving Configuration Data to Another Operating System" on page 76 for export/import information.
  - Upgrade the OS version on the system.
  - Install Steel-Belted Radius v6.1 and import the XML configuration file.

Starting the RADIUS Server

Use the following command to start the RADIUS server manually.

cd *server-directory*
./sbrd start

If you change configuration settings for your Steel-Belted Radius server, you may need to restart Steel-Belted Radius to make the changes effective. As an alternative to issuing an sbrd stop command immediately followed by an sbrd start command, you can use the sbrd restart command to restart Steel-Belted Radius. When you issue the sbrd restart command, Steel-Belted Radius shuts down and then immediately starts the RADIUS server process.

cd *server-directory*
./sbrd restart

Stopping the RADIUS Server

Use the following commands to stop the RADIUS server:

cd *server-directory*
./sbrd stop

When you execute the sbrd stop command, Steel-Belted Radius allows its subsystems to complete outstanding work and release resources, and then stops the mkded (btrieve) and radius processes gracefully.

If Steel-Belted Radius fails to stop after you issue the sbrd stop command, you can use the optional force argument to terminate all subsystems immediately.

cd *server-directory*
./sbrd stop force

Displaying RADIUS Status Information

You can use the sbrd status command to display status information for the RADIUS process.

cd *server-directory*
./sbrd status

Figure 6 illustrates the output of the sbrd status command.

Figure 6: Output of sbrd status Command

```
> sbrd status
ecarter 25927 .mkded start

—— Shared Memory Segments ——
key            shmid      owner      perms   bytes      nattch   status
0x42545256     891968     ecarter    600     8000000    2

—— Semaphore Arrays ——
key            semid      owner      perms   nsems
0x42545256     167116     ecarter    660     250

ecarter 2066 radius sbr.xml
radius processes are running
radius state is running
radius status 1101

Aggregate state is running
```

Chapter 6

Verifying Native User Authentication

This chapter describes how to verify that Steel-Belted Radius is configured to support native user authentication. Verifying native user authentication is the first step in troubleshooting other authentication problems.

You should complete the steps in this chapter, even if you do not anticipating using native user authentication, so that you can verify Steel-Belted Radius is installed and configured correctly.

Before You Begin

- Verify that you have installed the Steel-Belted Radius server software and SBR Administrator on a Windows, Solaris, or Linux host.
- Review the Steel-Belted Radius documentation.

Configuring the Server

After you have installed the Steel-Belted Radius software on your computer and have added the appropriate license numbers, you must configure the software. The specific steps you must perform depend on your network's authentication and accounting needs.

A summary of the steps for configuring Steel-Belted Radius is as follows.

1. Configure each of your RADIUS client devices to communicate with your Steel-Belted Radius server. To do this, you must log into each device and run its configuration interface.

2. Run the SBR Administrator program.

   You start the SBR Administrator by running a browser and opening a connection to the Steel-Belted Radius server you want to configure.

   To open a connection on a local host listening on port 1812, use the following URL:

http://localhost:1812/sbr/index.html

To open a connection on a remote host listening on port 1812, use the following URL, where *ipaddress* is the IP address or DNS name of the remote server:

http://*ipaddress*:1812/sbr/index.html

When the Steel-Belted Radius Administrator page opens, click the **Launch** link to download and start the SBR Administrator. You are then prompted to log in by entering your user credentials.

3. Use the RADIUS Clients panel to configure the server to communicate with each RADIUS client.

4. Use the Users panel to identify the users or groups of users who are permitted to access the RADIUS clients.

   Specify user attributes by selecting them in the Users panel or by creating user profiles in the Profiles dialog.

For more information, refer to the *Steel-Belted Radius Administration Guide*.

Verifying Native User Authentication

To verify native user authentication, you will need to download, install, and configure the RadiusTest utility.

Downloading the RadiusTest Utility

To download the RadiusTest utility:

1. Use a browser to point to the Steel-Belted Radius Technical Notes page (http://www.juniper.net/customers/support/products/aaa_802/sbr_kb.html).

2. Click the **Search** link.

3. When the Full Text Search window opens, enter **RD562** in the **Search** field and click the **Search** button.

4. Click the link for **Tech Note RD562** to open the "How to test SBR in Stand alone mode" technical note.

5. Scroll to the bottom of the technical note and click the **newtestr.zip** link.

6. When the File Download window opens, click **Save** and specify where to save the newtestr.zip file.

Installing the RadiusTest Utility

To install the RadiusTest utility:

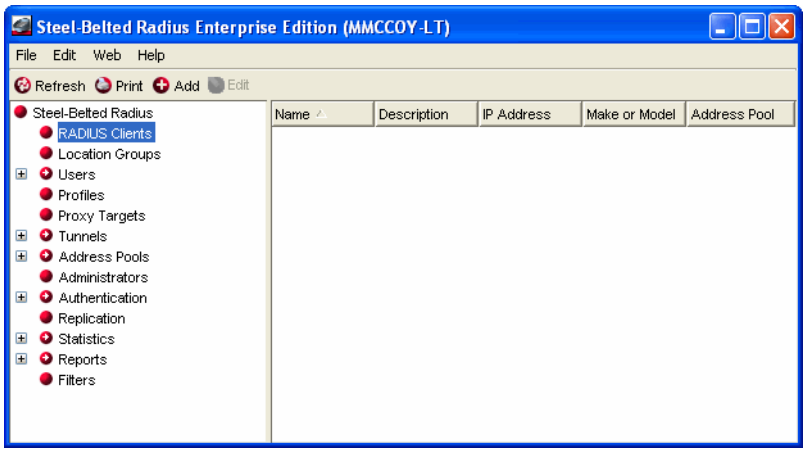
1. Create a directory called /radiustest in the /Program Files/Juniper Networks/Steel-Belted Radius directory on your computer.
2. Navigate to where you installed the newtestr.zip file on your hard disk.
3. Double-click the newtestr.zip file icon to open the file archive.
4. Copy the four files in the file archive to the /Program Files/Juniper Networks/Steel-Belted Radius/radiustest/ directory.

Configuring Steel-Belted Radius

To configure Steel-Belted Radius to work with the RadiusTest utility:

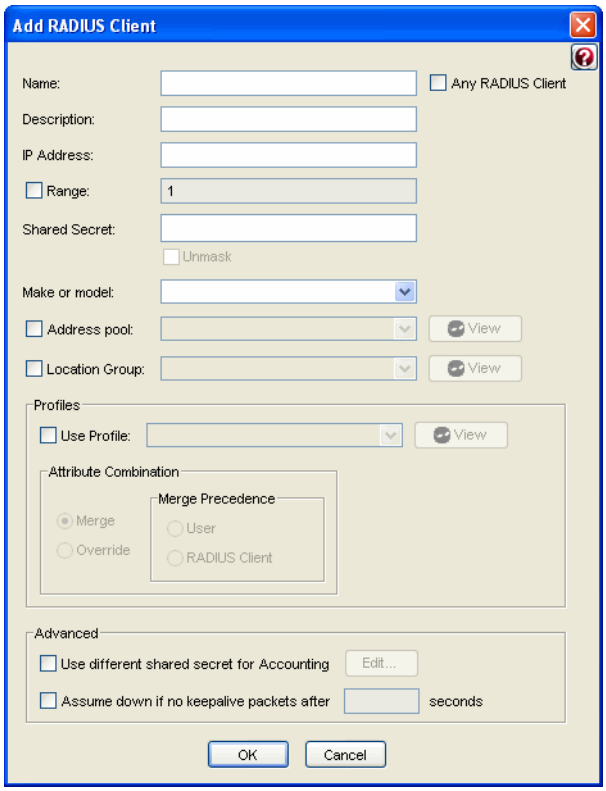
1. Run the SBR Administrator.
2. Log into the SBR Administrator using your username and password.
3. Click the **RADIUS Clients** button to open the RADIUS Clients panel (Figure 7).

Figure 7: RADIUS Clients Panel



4. Click the **Add** button to open the Add RADIUS Client window (Figure 8).

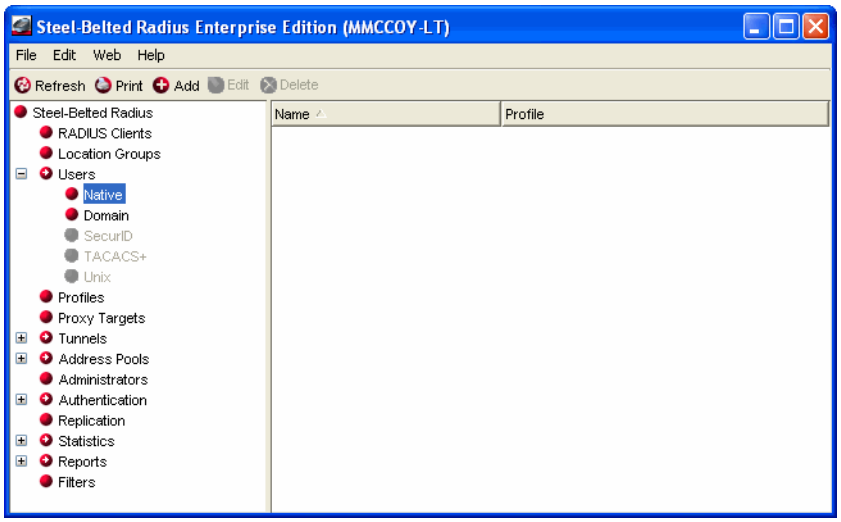
Figure 8: Add RADIUS Client Window



5. Configure your computer as a RADIUS client entry by entering the name of your computer in the **Name** field and the IP address of your computer in the **IP Address** field. Enter radius in the Shared Secret field. Click **OK**.

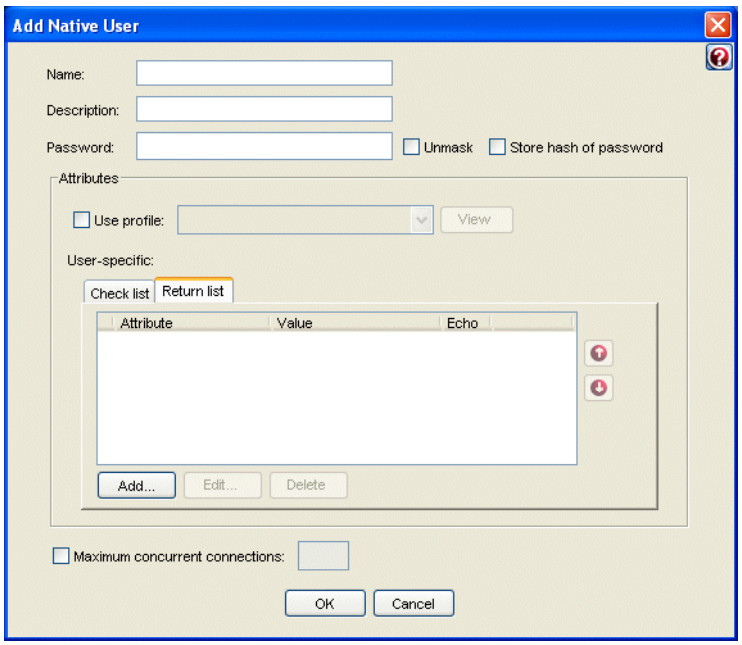
6. Click the **Users** > **Native** button to open the Native Users panel (Figure 9).

Figure 9: Native Users Panel



7. Click the **Add** button to open the Add Native User window (Figure 10).

Figure 10: Add Native User Window



8. Configure a test user by entering a name (testuser) and a password (testpw). Click **OK**.

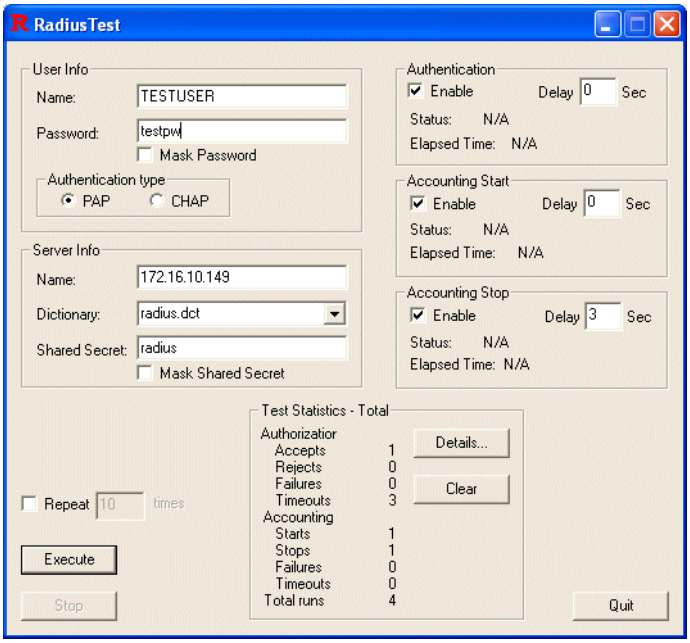
Configuring the RadiusTest Utility

To configure the RadiusTest utility:

1. Run the radiustest.exe application.

   The RadiusTest window (Figure 11) opens.

Figure 11: RadiusTest Window



2. Enter the settings for your test user in the **User Info** fields.

   a. Enter the user name to be sent in the RADIUS authentication request (TESTUSER) in the **Name** field.

   b. Enter the user password (testpw) in the **Password** field.

   c. Specify an authentication type.

      If you select PAP, the user password is sent in a decodable format.

      If you select CHAP, the user password is hashed before being sent to the Steel-Belted Radius server.

3. Enter the settings for the Steel-Belted Radius server running on your computer in the **Server Info** fields.

   a. Enter the name or IP address of your computer in the **Name** field.

   b. Leave the **Dictionary** list set to radius.dct.

   c. Enter the shared secret (radius) in the **Shared Secret** field. This must be the same value you configured when you set up the RADIUS client.

4. Optionally, use the **Authentication** controls to specify whether you want to send an authentication request for the specified user to the Steel-Belted Radius server and to specify how long you want the RadiusTest utility to delay before sending the request.

   The information sent in the authentication request can be customized by modifying the [Auth-Attribs] section of the radtest.ini file.

5. Optionally, use the **Accounting Start** and **Accounting Stop** controls to specify whether you want to send accounting start and stop requests for the specified user to the Steel-Belted Radius server and how long you want the RadiusTest utility to delay before sending the request.

   The information sent in the accounting request can be customized by modifying the [Acct-Start-Attribs] and [Acct-stop-Attribs] sections of the radtest.ini file.

6. Click the **Execute** button.

If native user authentication is configured properly, the **Authorization** and **Accounting** counters reflect successful authentication and accounting start messages.

If you click the **Details** button, the RadiusTest Details window displays the results of the most recent transaction.

```
RadTest Initialized - Socket bound
|||||||||||||||||||||||||||||| SessionStarting
||||||||||||||||||||||||||||||
Fixup attribute 5 = 0x8
>>> Authentication...
------ Packet: AUTH REQUEST   Length: 62 ------
User-Name = TESTUSER
User-Password = Encrypted 16 bytes:
 <80> <E8> <77> <D3> <2E> <DA> <7D> <F5> <CF> <CE> <4C> <63> <EB> <2B>
<6A> <A4>
NAS-IP-Address = 1.2.3.4
NAS-Port = 0x00000008
NAS-Port-Type = 0x00000002
-----------------------------------
>>> Sending Request id = 12 NAS = NAS DEFAULT
<<< Response Received for id = 12 NAS = NAS DEFAULT
------ Packet: AUTH ACCEPT   Length: 74 ------
Class = SBR
-----------------------------------
Fixup attribute 5 = 0x8
>>> Accounting Start...
------ Packet: ACCT REQUEST   Length: 119 ------
User-Name = TESTUSER
NAS-IP-Address = 1.2.3.4
NAS-Port = 0x00000008
NAS-Port-Type = 0x00000002
Acct-Status-Type = 0x00000001
Acct-Delay-Time = 0x00000064
Acct-Session-Id = 1234567
Class = SBR
-----------------------------------
>>> Sending Request id = 13 NAS = NAS DEFAULT
<<< Response Received for id = 13 NAS = NAS DEFAULT
------ Packet: ACCT RESPONSE   Length: 20 ------
-----------------------------------
Fixup attribute 5 = 0x8
>>> Accounting Stop...
------ Packet: ACCT REQUEST   Length: 119 ------
User-Name = TESTUSER
NAS-IP-Address = 1.2.3.4
```

```
NAS-Port = 0x00000008
NAS-Port-Type = 0x00000002
Acct-Status-Type = 0x00000002
Acct-Delay-Time = 0x00000064
Acct-Session-Id = 1234567
Class = SBR
---------------------------------
>>> Sending Request id = 14 NAS = NAS DEFAULT
<<< Response Received for id = 14 NAS = NAS DEFAULT
------ Packet: ACCT RESPONSE   Length: 20 ------
---------------------------------
Auth Time = 0 ms Acct Start Time = 0 ms Acct Stop Time = 0
|||||||||||||||||||||||||||||||| End of Pass
||||||||||||||||||||||||||||||||
|||||||||||||||||||||||||||||||| SessionFinished
||||||||||||||||||||||||||||||||
Authentication: Total = 1  Accept = 1  Reject = 0
    Failures = 0  Retries = 0  Timeouts = 0
Accounting : Starts 1  Stops 1
    Failures = 0  Retries = 0  Timeouts = 0
Average Response Times : Auth = 0  Acct Start = 0  Acct Stop = 0
```

Chapter 7

Uninstalling Steel-Belted Radius

This chapter describes how to uninstall the Steel-Belted Radius server software and the SBR Administrator from a Windows, Solaris, or Linux host.

Uninstalling on Windows

Use the Windows Add or Remove Programs control panel to uninstall the Steel-Belted Radius server software and SBR Administrator.

Uninstalling the Steel-Belted Radius Server

To uninstall the Steel-Belted Radius server software from a Windows host:

1. Choose **Start > Control Panel > Add or Remove Programs**.
2. When the Add or Remove Programs window opens, select **Steel-Belted Radius**.
3. Click **Remove**.
4. When a window asking you to confirm you want to remove Steel-Belted Radius opens, click **Yes**.
5. After the control panel indicates the Steel-Belted Radius server software has been uninstalled, archive or delete files remaining in the C:\Program Files\Juniper Networks\Steel-Belted Radius\Service directory.

Uninstalling the SBR Administrator Files

When you run the SBR Administrator, the application downloads and saves a number of files in your user folder. To uninstall the SBR Administrator files from a Windows host:

1. Exit the SBR Administrator. If you have more than one copy of SBR Administrator running, exit all copies.
2. Open the directory where your SBR Administrator files are stored.

   By default, this is C:\Documents and Settings*username*\Application Data\Juniper Networks.

3. Delete the \WebDeployer directory.

When you run the SBR Administrator application after you delete the \WebDeployer directory, it automatically downloads the files it needs from the appropriate Steel-Belted Radius server.

Uninstalling on Solaris

This section describes how to uninstall the SNMP agent, Steel-Belted Radius server software, and SBR Administrator configuration application on a Solaris host.

NOTE: You should not uninstall Steel-Belted Radius if you intend to install a later version of the Steel-Belted Radius software on the same server. Doing so will make it impossible to migrate your current data and configuration information.

Uninstalling the Steel-Belted Radius Server

To uninstall the Steel-Belted Radius server software from its default location (/opt/JNPRsbr):

1. Log into the Solaris server as root.

2. Stop the radius process by issuing the following commands:

```
# cd /opt/JNPRsbr/radius
# ./sbrd stop
```

3. Back up your Steel-Belted Radius server directory.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup.

```
# cd /opt/JNPRsbr
# mkdir /opt/backups
# tar cf - radius | ( cd /opt/backups; tar xfBp - )
```

4. Display the list of Steel-Belted Radius software packages installed on your server by typing the following command:

```
# cd /opt/JNPRsbr/radius
# pkginfo -x |egrep "JNPR|sbr"
JNPRsbrge    JNPRsbrge - Juniper Networks Steel-Belted Radius (Global
      Enterprise Edition)
```

5. Unconfigure the Steel-Belted Radius software by issuing the following command:

```
# cd /opt/JNPRsbr/radius/install
# ./unconfigure
```

6. Initiate the software uninstall by typing the pkgrm JNPRsbrxx command

   where *xx* represents the edition of Steel-Belted Radius you want to uninstall (ge, sp, or ee).

   When you are prompted to confirm you want to remove the package, enter **y**.

   ```
   # pkgrm JNPRsbrge

   The following package is currently installed:
     JNPRsbrge       JNPRsbrge - Juniper Networks Steel-Belted Radius (Global
       Enterprise Edition) (sparc) 6.1.0000

   Do you want to remove this package? y
   ## Removing installed package instance <JNPRsbrge>

   This package contains scripts which will be executed with super-user
       permission during the process of removing this package.

   Do you want to continue with the removal of this package [y,n,?,q] y
   ```

   After you confirm you want to continue, the uninstaller displays the name of each file it removes. The uninstall is complete when you see the following:

   ```
   Removal of <JNPRsbrge> was successful.
   ```

7. Optionally, remove the Steel-Belted Radius backup directories.

   ```
   # cd /
   # rm -rf /opt/JNPRsbr
   ```

Uninstalling the SBR Administrator Files

When you run the SBR Administrator, the application downloads and saves a number of files in your user folder. To uninstall the SBR Administrator files from a Solaris host:

1. Exit the SBR Administrator. If you have more than one copy of SBR Administrator running, exit all copies.

2. Issue the following command:

   ```
   rm –r -f $HOME/.junipernetworks/WebDeployer
   ```

If you run the SBR Administrator after you delete the /WebDeployer directory, your browser automatically downloads the files it needs to run SBR Administrator from the target Steel-Belted Radius server.

Uninstalling on Linux

This section describes how to uninstall the Steel-Belted Radius server software and SBR Administrator configuration application on a Linux host.

NOTE: You should not uninstall Steel-Belted Radius if you intend to install a later version of the Steel-Belted Radius software on the same server. Doing so will make it impossible to migrate your current data and configuration information.

Uninstalling the Steel-Belted Radius Server

To uninstall the Steel-Belted Radius server software from its default location (/opt/JNPRsbr):

1. Log into the Solaris server as root.

2. Stop the radius process by issuing the following commands:

   ```
   # cd /opt/JNPRsbr/radius
   # ./sbrd stop
   ```

3. Back up your Steel-Belted Radius server directory.

   You want to create a new archive directory to ensure that you do not overwrite an existing backup.

   ```
   # cd /opt/JNPRsbr
   # mkdir /opt/backups
   # tar cf - radius | ( cd /opt/backups; tar xfBp - )
   ```

4. If you are uninstalling the SNMP module, stop all SNMP agents currently running on your server.

5. Unconfigure the Steel-Belted Radius software by issuing the following commands:

   ```
   # cd /opt/JNPRsbr/radius/install
   # ./unconfigure
   ```

6. Execute the following command to uninstall the Steel-Belted Radius server software:

   # rpm -e sbr-*edition*-6.1.0-0

   where *edition* specifies the version of Steel-Belted Radius (Global Enterprise Edition (gee); Service Provider Edition (spe); Enterprise Edition (ee)) and version specifies the software version you want to install. For example, to run the RPM package used to uninstall the GEE version of Steel-Belted Radius version 6.1, you would enter the following:

   # rpm -e sbr-gee-6.1.0-0

The uninstall script archives all current configuration files, database files, and data files to the /install/backups/*timestamp* directory and deletes Steel-Belted Radius from your server.

7. Optionally, remove the Steel-Belted Radius backup directories.

```
# cd /
# rm -rf /opt/JNPRsbr
```

Uninstalling the SBR Administrator Files

When you run the SBR Administrator, the application downloads and saves a number of files in your user folder. To uninstall the SBR Administrator files from a Linux host:

1. Exit the SBR Administrator. If you have more than one copy of SBR Administrator running, exit all copies.

2. Issue the following command:

```
rm –r -f $HOME/.junipernetworks/WebDeployer
```

If you run the SBR Administrator after you delete the /WebDeployer directory, your browser automatically downloads the files it needs to run SBR Administrator from the target Steel-Belted Radius server.

Glossary

802.1X	The IEEE 802.1X standard defines a mechanism that allows a supplicant (client) to connect to a wireless access point or wired switch (authenticator) so that the supplicant can provide authentication credentials that can be verified by an authentication server.
AAA	Authentication, authorization, and accounting.
accounting	The process of recording and aggregating resource use statistics and log files for a user, connection session, or function for billing, system diagnosis, and usage planning.
agent	SNMP module on a managed device that responds to requests from a management station and sends traps to one or more recipients (trap sinks) to inform administrators of potential problems.
AP	Access Point. A device that serves as a communication hub to connect 802.1X wireless clients to a wired network.
attribute	RADIUS attributes carry the specific authentication, authorization, and accounting.
authentication	The process of verifying the identity of a person or file system and whether the person is allowed on a protected network.
authentication server	A back-end database server that verifies, from the credentials provided by an access client, whether the access client is authorized to use network resources.
authorization	The process of controlling the access settings, such as privileges and time limits, that the user can exercise on a protected network.
AVP	Attribute-value pair. An attribute and its corresponding value; for example, User-Name=admin.
blacklist	A profile of checklist attributes that cause Steel-Belted Radius to reject an authentication request. For example, a blacklist profile might specify calling station phone numbers or IP addresses that are blocked by Steel-Belted Radius.
CA	Certificate authority. A trusted entity that registers the digital identity of a site or individual and issues a digital certificate that guarantees the binding between the identity and the data items in a certificate.
CCM	Centralized configuration management. The process by which information is shared between a primary RADIUS server and one or more replica RADIUS servers in a multi-server environment.
certificate	A digital file signed by a CA that guarantees the binding between an identity and the contents of the certificate.
CHAP	Challenge Handshake Authentication Protocol. An authentication protocol where a server sends a challenge to a requestor after a link has been established. The requestor responds with a value obtained by executing a hash function. The server

verifies the response by calculating its own hash value: if the two hash values match, the authentication is acknowledged.

checklist — A list of attributes that must accompany a request for connection before the connection request can be authenticated.

CIDR — Classless Inter-Domain Routing. In CIDR notation, an IP address is represented as A.B.C.D/n, where /n identifies the IP prefix or network prefix). The IP prefix identifies the number of significant its used to identify a network. For example, 192.168.1.22/18 means "use the first 18 bits to represent the network and the remaining 14 bits to identify hosts." Common prefixes are /8 (Class A network), /16 (Class B network), /24 (Class C network), and /32.

Table 10: CIDR Translation

CIDR Format	First Address	Last Address	Number of Usable IP Addresses[a]	Comparable IP Subnet Mask
10.0.0.0/8	10.0.0.0	10.255.255.255	16,777,214	255.0.0.0
10.0.0.0/16	10.0.0.0	10.0.255.255	65,534	255.255.0.0
192.168.0.0/24	192.168.0.0	192.168.0.255	254	255.255.255.0
192.168.0.0/25	192.168.0.0	192.168.0.127	126	255.255.255.128
192.168.0.0/26	192.168.0.0	192.168.0.63	62	255.255.255.192
192.168.0.0/27	192.168.0.0	192.168.0.31	30	255.255.255.224
192.168.0.0/28	192.168.0.0	192.168.0.15	14	255.255.255.240
192.168.0.0/29	192.168.0.0	192.168.0.7	6	255.255.255.248
192.168.0.9/29	192.168.0.8	192.168.0.15	6	255.255.255.248
192.168.0.10/30	192.168.0.8	192.168.0.11	2	255.255.255.252
192.168.0.10/31	192.168.0.10	192.168.0.11	0	255.255.255.254
192.168.0.10/32	192.168.0.10	192.168.0.10	1	255.255.255.255

a. Excludes the first address (network address) and last address (broadcast address) in an address range.

community — An SNMP community is a group of devices and management stations running SNMP. An SNMP device or agent may belong to more than one SNMP community.

community string — Character string included in SNMP messages to identify valid sources for SNMP requests and to limit access to authorized devices.

- The read community string allows an SNMP management station to issue Get and GetNext messages.
- The write community string allows an SNMP management station to issue Set messages.

credentials — Data that is verified when presented to an authenticator, such as a password or a digital certificate.

CRL — Certificate Revocation List. A data structure that identifies the digital certificates that have been invalidated by the certificates' issuing CA prior to their expiration date.

daemon — *See* process.

dictionary	Text file that maps the attribute/value pairs supported by third-party RADIUS vendors.
DHCP	Dynamic Host Configuration Protocol. Protocol by which a server automatically assigns (leases) a network address and other configuration settings to a client temporarily or permanently.
DNIS	Dialed number identification service. A telephone service that identifies what number was dialed by a caller.
DNS	Domain Name Service. Internet protocol for mapping host names, domain names, and aliases to IP addresses.
EAP	Extensible Authentication Protocol. An industry-standard authentication protocol for network access that acts as a transport for multiple authentication methods or types. Defined by RFC 2284.
EAP-32	*See* POTP.
EAP-FAST	Authentication method that uses EAP (Extensible Authentication Protocol) and FAST (Flexible Authentication via Secure Tunneling).
EAP-TLS	Authentication method that uses EAP (Extensible Authentication Protocol) and TLS (Transport Layer Security).
EAP-TTLS	Authentication method that uses EAP (Extensible Authentication Protocol) and TTLS (Tunneled Transport Layer Security).
GTC	Generic Token Card.
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force. Technical subdivision of the Internet Architecture Board that coordinates the development of Internet standards.
IPv4	Implementation of the TCP/IP suite that uses a 32-bit addressing structure.
IPv6	Implementation of the TCP/IP suite that uses a 128-bit addressing structure.
Java	Programming language designed for use in distributed environments such as the Internet.
JDBC	Java Database Connectivity. Application programming interface for accessing a database from programs written in Java.
LDAP	Lightweight Directory Access Protocol. An IETF standard protocol for updating and searching directories over TCP/IP networks.
LDIF	LDAP Data Interchange Format. The format used to represent directory server entries in text form.
LEAP	Lightweight Extensible Authentication Protocol.
MAC	(1) Message Authentication Code. A MAC function takes a variable-length input and a key to produce a fixed-length output to carry authentication and integrity protection of data. (2) Media Access Control. The unique hardware address associated with a computer network interface.
managed device	A device that runs an SNMP agent.
management station	Host that monitors and controls managed devices running SNMP agents.
MIB	Management Information Base. A database of objects, such as alarm status or statistics counters, that can be monitored or overwritten by an SNMP management station.

MPPE	Microsoft Point-to-Point Encryption. A means of representing point-to-point packets in an RC4 encrypted format. Defined in RFC 3078.
MS-CHAP	Microsoft CHAP. Proprietary version of CHAP.
NAD	Network Access Device. Any device that accepts connection requests from remote users, authenticates users through RADIUS, and routes user onto the network. Identical in meaning to remote access server (RAS) and network access server (NAS).
NAT	Network Address Translation. Technique that allows an intranet to use IP addresses that are different from what the outside Internet thinks
native user	A user authenticated by Steel-Belted Radius using its internal authentication database.
ODBC	Open Database Connectivity. Standard (open) application programming interface for accessing a database.
OTP token	One-time password token. Hardware or software module that generates one-time passwords that can be used to authenticate a user.
PAC	Protected Access Credential. A high-entropy secret that is known to both the RADIUS client and the RADIUS server to secure the TLS handshake in EAP-FAST authentication.
PAP	Password Authentication Protocol. An authentication protocol where a requestor sends an identifier and password to a server after a link has been established. If the identifier and password match an entry in the server's database, the authentication is acknowledged.
PEAP	Protected Extensible Authentication Protocol. A two-phase authentication protocol where (1) an authentication server is authenticated to a supplicant using a digital certificate and a secure channel is established; and (2) the supplicant is authenticated to the authentication server through the secure channel.
POTP	Protected One-Time Password. EAP method that uses one-time password tokens for unilateral or mutual authentication.
process	A program on a Solaris or Linux host that runs continuously to handle service requests. Sometimes referred to as a daemon.
proxy RADIUS	Process of authenticating users whose profiles are on other RADIUS servers by forwarding access-request packets received from a RADIUS client to a remote RADIUS server (the proxy target), and then forwarding the response from the remote server back to the RADIUS client.
proxy target	The remote RADIUS server that actually performs authentication in a proxy RADIUS sequence.
RADIUS	Remote Authentication Dial In User Service. A client/server security administration standard that functions as an information clearinghouse, storing authentication information about users and administering multiple security systems across complex networks.
RAS	Remote Access Server. *See* network access device.
return list	A list of attributes that Steel-Belted Radius must return to a RADIUS client after authentication of a user succeeds. The return list usually provides additional parameters that the RADIUS client needs to complete the connection.
roaming	The ability to move from one Access Point coverage area to another without interruption of service or loss of connectivity.

RSA SecurID	Security token system that allows remote-access users to generate a pseudorandom value they can forward as part of an authentication sequence.
session ID	Session Identifier. A string of characters uniquely identifying the session.
SHA-1	Secure Hash Algorithm-1. A one-way cryptographic function that takes a message of any length and produces a 160-bit message digest.
shared secret	An encryption key known only to the sender and receiver of data.
silent discard	The process of discarding a packet without further processing and without notification to the sender.
SNMP	Simple Network Management Protocol.
SSL	Secure Sockets Layer. Program layer that manages the security of messages on a network.
supplicant	The client in an 802.1X-authenticated network.
TACACS +	Terminal Access Controller Access Control System (with enhancements). An authentication protocol that allows a RAS to communicate with an authentication server to determine if a user should have access to a protected network.
TLS	Transport Layer Security.
trap	An SNMP message that reports a significant event, such as a problem, error, or change in state, that occurred within a managed device.
trap sink	The destination for trap messages sent by an SNMP agent on a managed device.
TTLS	Tunneled Transport Layer Security.
user database	A database where a RADIUS server keeps information about users, such as authentication information and network access permissions.
user profile	A record in the user database that describes how a particular user or class of users should be configured during authentication and authorization.
VSA	Vendor Specific Attributes.
WEP	Wired Equivalent Privacy. An encryption method designed to encrypt traffic between a WLAN client and an access point.
WLAN	Wireless Local Area Network.

Index

Numerics

802.1X....1

A

Add a License for Server window....18, 33, 58
auto-restart....11, 12

D

Database migration
  Linux....67
  Windows....20
dbconvert utility....67
directed authentication....2
DNIS....2

F

force....49, 79

I

IAS....15
Install
  Linux, new install....53
  Linux, upgrade....59
  Solaris, new install....27
  Solaris, upgrade....34
  Windows, new install....15
  Windows, upgrade....19
install_sbradmin_sol.sh command....47
Internet Authentication Service, see IAS

L

LDAP....1
license number....18, 28, 33, 41, 54, 58, 66
License, Solaris note....33

M

memory....8, 10, 12
Microsoft IAS....15
Migrate existing configuration database
  Linux (dbconvert)....67
  Windows....20
Move SBR to a new OS....75
  export data....76
  import data....77
  manual copy....77
  move configuration data....76

O

ODBC compliant....9, 11
Open Database Connectivity....9, 11
Operating system migration
  Linux....75, 78
Oracle....9, 11

P

Perfmon....2
Perl....11, 12
process, RADIUS....39, 64
proxy RADIUS....1

R

RADIUS daemon....39, 64
radiusdir....ix
radtest.ini....86

S

SBR Administrator....8, 10, 12
  uninstall old version, Linux....74
  uninstall old version, Solaris....47
  uninstall old version, Windows....23
sbrd....90, 92
sbrd restart....49, 79
sbrd start....49, 77, 78
sbrd status....49, 79
sbrd stop....49, 76, 79
sbrd stop force....49, 79
SNMP....2, 25, 51
SQL....1
SQL database....9, 11
stop force....49, 79

T

Test utility....82

U

Uninstall
  Linux....92
  Solaris....90
  Windows....89
uninstall....47
Upgrade
  Linux platforms....59
  scenarios, Linux 5.4....62
  scenarios, Linux 6.0....63
  scenarios, Solaris 5.4....37

scenarios, Solaris 6.0 38
Solaris platforms 34
Windows platforms 19

V

Verify native user authentication 82